EVROPSKÁ
KOMISE

V Bruselu dne 11.4.2024
C(2024) 2393 final

DOPORUČENÍ KOMISE

ze dne 11.4.2024

o plánu pro koordinovanou implementaci přechodu na postkvantovou kryptografii

DOPORUČENÍ KOMISE

ze dne 11.4.2024

o plánu pro koordinovanou implementaci přechodu na postkvantovou kryptografii

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie, a zejména na článek 292 této smlouvy,

s ohledem na směrnici Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148[1] (směrnice NIS 2),

vzhledem k těmto důvodům:

(1) Ochrana údajů a zabezpečení citlivých komunikací mají zásadní význam pro společnost, hospodářství, bezpečnost a prosperitu Unie. Kybernetická bezpečnost má strategický význam při vytváření „Evropy připravené na digitální věk“[2] a je klíčovým cílem politického programu Digitální dekáda[3].

(2) Strategie bezpečnostní unie EU[4] i Strategie kybernetické bezpečnosti EU[5] zdůrazňují šifrování jako klíčovou technologii pro dosažení odolnosti a technologické suverenity a pro budování operační kapacity za účelem předcházení kybernetickým útokům. Šifrování má v digitálním světě zásadní význam pro zabezpečení digitálních systémů a transakcí, pro ochranu řady základních práv, jakož i pro zabezpečení obranných schopností. Soutěžení různých zemí a soukromých subjektů za účelem rozvoje kapacit v oblasti kvantové výpočetní techniky a vytváření nových potenciálně výhodných příležitostí představuje hrozbu pro stávající kryptografické normy. Tyto normy hrají klíčovou úlohu při zajišťování důvěrnosti a integrity údajů a ochrany citlivých komunikací, jakož i při podpoře základních prvků bezpečnosti sítí.

(3) Budoucí potenciální vývoj kvantových počítačů schopných prolomit dnešní šifrování vyžaduje, aby Evropa hledala silnější záruky a zajistila ochranu citlivých komunikací a dlouhodobou integritu důvěrných informací, tj. aby co nejrychleji přešla na postkvantovou kryptografii. Tento nový typ kryptografie odstraní známé slabiny současné asymetrické kryptografie a posílí odolnost vůči hrozbám, které představuje zneužívání kvantových počítačů.

(4) Komise financuje výzkum a vývoj postkvantové kryptografie již více než deset let, přičemž uznává potenciální hrozbu, kterou kvantová výpočetní technika představuje pro současnou kryptografii s veřejným klíčem.

---

1 Úř. věst. L 333, 27.12.2022, s. 80.
2 COM(2020) 67 final.
3 Rozhodnutí Evropského parlamentu a Rady (EU) 2022/2481 ze dne 14. prosince 2022, kterým se zavádí politický program Digitální dekáda 2030 (Úř. věst. L 323, 19.12.2022, s. 4).
4 COM(2020) 605 final.
5 JOIN(2020) 18 final.

(5) Členské státy by měly zvážit co nejrychlejší přechod svých stávajících digitálních infrastruktur a služeb pro orgány veřejné správy a další kritické infrastruktury na postkvantovou kryptografii, který by vedl k zásadnímu posunu v šifrovacích algoritmech, protokolech a systémech. Jak se zdůrazňuje v nedávno zveřejněné bílé knize Komise nazvané „Jak zvládnout potřeby Evropy v oblasti digitální infrastruktury?“, je zapotřebí koordinovaného úsilí za účasti vládních agentur, normalizačních orgánů, zainteresovaných stran z odvětví, výzkumných pracovníků a odborníků v oblasti kybernetické bezpečnosti.

(6) Toto doporučení Komise vybízí členské státy k tomu, aby vypracovaly komplexní strategii pro přijetí postkvantové kryptografie s cílem zajistit koordinovaný a synchronizovaný přechod mezi jednotlivými členskými státy a jejich veřejným sektorem. Strategie by měla stanovit jasné cíle, milníky a harmonogramy, které povedou k vymezení společného plánu pro koordinovanou implementaci postkvantové kryptografie. Výsledkem by mělo být zavedení technologií postkvantové kryptografie do stávajících systémů veřejné správy a kritických infrastruktur v celé Unii prostřednictvím hybridních systémů, které mohou postkvantovou kryptografii kombinovat se stávajícími šifrovacími přístupy nebo s kvantovou distribucí klíče.

(7) V zájmu účinného přechodu na postkvantovou kryptografii by měl plán pro koordinovanou implementaci postkvantové kryptografie obsahovat seznam opatření, jimiž se mají členské státy zabývat, včetně zvážení algoritmů postkvantové kryptografie, s jasným harmonogramem pro různé fáze a milníky, jichž má být dosaženo, s přihlédnutím k jejich vzájemné závislosti, jakož i k zúčastněným stranám, které se mají zapojit.

(8) Pro harmonizované provádění postkvantové kryptografie v celé Unii je nezbytné vypracovat společné evropské normy a rámec pro identifikaci a výběr algoritmů postkvantové kryptografie, které mají být zavedeny v digitálních sítích a službách v celé Unii. Prostřednictvím aktivní účasti výzkumných pracovníků financovaných EU již Unie podporuje vývoj a testování kandidátů na algoritmus postkvantové kryptografie pro účely norem v mezinárodních postupech výběru postkvantové kryptografie. Toto doporučení Komise vybízí členské státy k úzké spolupráci na úrovni EU s odborníky Unie na kybernetickou bezpečnost, se skupinou pro spolupráci v oblasti bezpečnosti sítí a informací a s Agenturou Evropské unie pro kybernetickou bezpečnost (ENISA) při hodnocení a výběru vhodných algoritmů postkvantové kryptografie a jejich přijetí jako norem EU pro harmonizované používání v celé Unii.

(9) Členské státy a Unie by měly i nadále aktivně spolupracovat se svými mezinárodními strategickými partnery na vývoji mezinárodních norem v oblasti postkvantové kryptografie s cílem zajistit interoperabilitu komunikací do budoucna.

(10) Jakmile se členské státy na plánu pro koordinovanou implementaci postkvantové kryptografie dohodnou, měl by plán sloužit jako návrh pro vymezení vnitrostátních plánů přechodu na postkvantovou kryptografii, nebo pokud vnitrostátní plány existují, pro jejich sladění se společným plánem pro koordinovanou implementaci postkvantové kryptografie.

(11) Komise má v úmyslu pečlivě sledovat opatření přijatá v reakci na toto doporučení, aby bylo zajištěno dosažení pokroku v plnění jeho cílů. Členské státy se proto vybízejí, aby Komisi na její žádost předložily veškeré relevantní informace, jejichž poskytnutí lze v zájmu zajištění tohoto sledování důvodně očekávat. Na základě takto získaných informací a všech dalších dostupných informací Komise posoudí účinky tohoto

doporučení a určí, zda jsou zapotřebí další kroky, včetně navržení právně závazných aktů Unie.

(12) Toto doporučení o postkvantové kryptografii vychází z politických cílů stanovených ve Strategii kybernetické bezpečnosti EU pro zlepšení celkového zabezpečení a odolnosti digitálních infrastruktur a služeb Unie pro orgány veřejné správy a další kritické infrastruktury, slouží cílům jednotného digitálního trhu a společného sdělení o Strategii evropské hospodářské bezpečnosti (10919/23)[6] a bere v úvahu rizika pro fyzickou a kybernetickou bezpečnost kritických infrastruktur, jakož i rizika zjištěná v rámci nedávno provedeného posouzení rizik pro kvantové technologie[7]. Dodržuje základní práva a ctí zásady uznané zejména Listinou základních práv EU (články 7, 8 a 11) a Evropskou úmluvou o lidských právech (články 8 a 10), z nichž vyplývá pozitivní povinnost vlád minimalizovat riziko neoprávněného přístupu k informacím a kontroly nad nimi, což vyžaduje ochranu a podporu kryptografických technologií,

PŘIJALA TOTO DOPORUČENÍ:

1. OBLAST PŮSOBNOSTI A CÍLE

Toto doporučení má za účel podpořit přechod na postkvantovou kryptografii za účelem ochrany digitálních infrastruktur a služeb pro orgány veřejné správy a další kritické infrastruktury v Unii tím, že členským státům umožní:

1) definovat „plán pro koordinovanou implementaci postkvantové kryptografie“, jehož cílem je synchronizovat úsilí členských států při navrhování a provádění vnitrostátních plánů přechodu a zároveň zajistit přeshraniční interoperabilitu;

2) podporovat hodnocení a výběr příslušných algoritmů postkvantové kryptografie EU s pomocí odborníků na kybernetickou bezpečnost a další přijímání takových algoritmů jako norem Unie, které by v rámci plánu pro koordinovanou implementaci postkvantové kryptografie měly být zavedeny v celé Unii;

3) přijmout vhodná a přiměřená opatření k přípravě na tento přechod.

2. PLÁN PRO KOORDINOVANOU IMPLEMENTACI ZABÝVAJÍCÍ SE PŘECHODEM NA POSTKVANTOVOU KRYPTOGRAFII

4) Toto doporučení vybízí členské státy, aby svá opatření na úrovni Unie koordinovaly prostřednictvím specializovaného fóra členských států. Komise za tímto účelem doporučuje, aby členské státy využily stávajících struktur v oblasti kybernetické bezpečnosti na úrovni Unie a zřídily podskupinu v rámci skupiny pro spolupráci v oblasti bezpečnosti sítí a informací. Tato podskupina by mohla zahrnovat zástupce národních bezpečnostních agentur a odborníky na kybernetickou bezpečnost, zejména z vnitrostátních orgánů pro kybernetickou bezpečnost a agentury ENISA. Podskupina může k účasti na své práci přizvat zástupce příslušných zainteresovaných stran, například zástupce poradních orgánů veřejných organizací, průmyslu, poskytovatelů služeb a provozovatelů, s cílem shromažďovat vstupy a vyměňovat si informace o přechodu digitálních infrastruktur a služeb pro orgány veřejné správy a dalších kritických infrastruktur na postkvantovou kryptografii v různých odvětvích, koordinovat jejich úsilí na vnitrostátní úrovni a vypracovat plán pro koordinovanou

[6] https://data.consilium.europa.eu/doc/document/ST-10919-2023-INIT/cs/pdf

[7] JOIN(2023) 20 final.

implementaci postkvantové kryptografie v souladu s pravidly Unie v oblasti hospodářské soutěže a právními předpisy Unie v oblasti ochrany údajů.

5) Tato podskupina pro postkvantovou kryptografii by měla zvážit vhodná, účinná a přiměřená opatření pro vymezení a koordinaci vypracování plánu pro koordinovanou implementaci postkvantové kryptografie. Podskupina pro postkvantovou kryptografii se vyzývá k zapojení do diskusí s dalšími relevantními orgány, jako je Europol, NATO nebo jiné, aby se zabránilo zdvojování úsilí a zajistil se soudržný přístup k řešení nově se objevujících výzev.

6) Za tímto účelem se členské státy vyzývají, aby krátce po zveřejnění tohoto doporučení zřídily tuto podskupinu pro postkvantovou kryptografii v souladu s prováděcím rozhodnutím Komise (EU) 2017/179 a aby jmenovaly zástupce odborníků, kteří by měli úzce spolupracovat s Komisí a kteří by měli být pověřeni vymezením a vypracováním plánu pro koordinovanou implementaci postkvantové kryptografie.

7) Plán pro koordinovanou implementaci postkvantové kryptografie by měl být k dispozici po uplynutí dvou let od zveřejnění tohoto doporučení; poté bude následovat vypracování a další přizpůsobení plánů přechodu na postkvantovou kryptografii jednotlivých členských států v souladu se zásadami stanovenými v plánu pro koordinovanou implementaci postkvantové kryptografie.

3. OPATŘENÍ NA ÚROVNI UNIE

8) Komise bude pravidelně sledovat a hodnotit celkovou práci ve spolupráci s odbornými zástupci členských států.

9) Komise může za tímto účelem zástupce členských států požádat, aby předložili veškeré relevantní informace, jejichž poskytnutí lze v zájmu zajištění sledování pokroku dosaženého při vypracovávání tohoto plánu pro koordinovanou implementaci postkvantové kryptografie a účinnosti těchto opatření důvodně očekávat.

10) Na základě těchto a všech dalších dostupných informací Komise navržená opatření a fungování sítě zástupců členských států posoudí a určí, zda jsou zapotřebí další kroky, včetně navržení právně závazných aktů Unie.

4. PŘEZKUM

11) Členské státy by měly spolupracovat s Komisí na posouzení účinků tohoto doporučení nejpozději tři roky po jeho zveřejnění s cílem určit další vhodné kroky. Toto posouzení by mělo zohlednit výsledek práce podskupiny národních odborníků pro postkvantovou kryptografii.

V Bruselu dne 11.4.2024

Za Komisi
Thierry BRETON
člen Komise

ÚŘEDNĚ OVĚŘENÝ OPIS
Za generální tajemnici

Martine DEPREZ
Ředitel
Rozhodování a jednání ve sboru
EVROPSKÁ KOMISE