SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY 2013/40/EU

ze dne 12. srpna 2013

o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV

EVROPSKÝ PARLAMENT A RADA EVROPSKÉ UNIE,

s ohledem na Smlouvu o fungování Evropské unie, a zejména na čl. 83 odst. 1 této smlouvy,

s ohledem na návrh Evropské komise,

po postoupení návrhu legislativního aktu vnitrostátním parlamentům,

s ohledem na stanovisko Evropského hospodářského a sociálního výboru [1],

v souladu s řádným legislativním postupem [2],

vzhledem k těmto důvodům:

(1) Cílem této směrnice je sblížit ustanovení trestního práva členských států v oblasti útoků na informační systémy prostřednictvím stanovení minimálních pravidel týkajících se definice trestných činů a příslušných sankcí a zlepšit spolupráci mezi příslušnými orgány, včetně policie a dalších specializovaných donucovacích orgánů členských států, jakož i mezi příslušnými specializovanými agenturami a institucemi Unie, jako je Eurojust, Europol a jeho Evropské centrum pro boj proti kyberkriminalitě a Evropská agentura pro bezpečnost sítí a informací (ENISA).

(2) Informační systémy jsou klíčovým prvkem politické, sociální a hospodářské interakce v Unii. Společnost je na takových systémech značně závislá a tato závislost se neustále zvyšuje. Hladké fungování a bezpečnost těchto systémů v Unii jsou nezbytné pro rozvoj vnitřního trhu a konkurenceschopného a inovativního hospodářství. Zajištění odpovídajících úrovní ochrany informačních systémů by mělo být součástí účinného komplexního rámce preventivních opatření doprovázejících kroky v oblasti trestního práva podnikané v reakci na kybernetickou kriminalitu.

(3) Útoky na informační systémy, zejména útoky spojené s organizovanou trestnou činností, představují rostoucí hrozbu jak v Unii, tak i v celosvětovém měřítku, a zvyšuje se obava z potenciálních teroristických anebo politicky motivovaných útoků na informační systémy, které jsou součástí kritické infrastruktury členských států a Unie. Tato skutečnost ohrožuje vytváření bezpečnější informační společnosti a oblasti svobody, bezpečnosti a práva, a proto je třeba na ni reagovat na úrovni Unie a dosáhnout intenzivnější spolupráce a koordinace na mezinárodní úrovni.

(4) V Unii existuje řada kritických infrastruktur, jejichž narušení nebo zničení by mělo závažné přeshraniční dopady. Z nutnosti zvýšit schopnost ochrany kritické infrastruktury v Unii je zřejmé, že opatření pro boj proti kybernetickým útokům by měla být doprovázena přísnými trestními sankcemi odpovídajícími závažnosti takových útoků. Kritickou infrastrukturou můžeme rozumět prostředky, systémy a jejich části nacházející se v členském státě, které jsou zásadní pro zachování nejdůležitějších společenských funkcí, zdraví, bezpečnosti, zabezpečení nebo dobrých hospodářských či sociálních podmínek obyvatel, jako jsou elektrárny, dopravní sítě nebo vládní sítě, a jejichž narušení nebo zničení by mělo pro členský stát závažný dopad v důsledku selhání těchto funkcí.

(5) Existují důkazy o směřování k čím dál tím nebezpečnějším a opakovaným rozsáhlým útokům na informačním systémy, které mají často kritický význam pro členské státy nebo pro konkrétní funkce ve veřejném nebo soukromém sektoru. Tuto tendenci doprovází rozvoj čím dál tím vyspělejších metod, jako je vytváření a používání tzv. „botnetů“, což se vyznačuje několika stádii trestného činu, kdy by každé samotné stádium mohlo představovat vážné nebezpečí pro veřejné zájmy. Tato směrnice usiluje mimo jiné o zavedení trestních sankcí za vytváření „botnetů“, tedy skutku, kdy na základě cílených kybernetických útoků dojde v důsledku napadení škodlivým softwarem k dálkovému ovládání značného počtu počítačů. Jakmile dojde k takovému propojení, může být napadená síť počítačů, která tvoří „botnet“, aktivována bez vědomí uživatelů počítačů s cílem spustit rozsáhlé kybernetické útoky, které jsou obvykle schopné způsobit závažnou škodu, jak je uvedeno v této směrnici. Členské státy by měly mít možnost stanovit, co se rozumí závažnou škodou podle jejich vnitrostátního práva a praxe, jako jsou například narušení systémových služeb značného veřejného významu, nebo vznik velkých finančních nákladů či způsobení ztrát osobních údajů nebo citlivých informací.

(6) Rozsáhlé kybernetické útoky mohou způsobit závažné hospodářské škody, a to jak v důsledku přerušení informačních systémů a komunikací, tak i v důsledku ztráty nebo pozměnění důvěrných informací nebo jiných údajů důležitých z obchodního hlediska. Zvláštní pozornost je třeba věnovat tomu, aby se v důsledku větší závislosti inovativních malých a středních podniků na řádném fungování a dostupnosti informačních systémů a často omezených zdrojů, jež mají k dispozici pro účely informační bezpečnosti, zvyšovalo jejich povědomí o hrozbách souvisejících s takovými útoky a jejich zranitelnosti vůči těmto útokům.

[1] Úř. věst. C 218, 23.7.2011, s. 130.

[2] Postoj Evropského parlamentu ze dne 4. července 2013 (dosud nezveřejněný v Úředním věstníku) a rozhodnutí Rady ze dne 22. července 2013.

(7) Pro zajištění konzistentního přístupu členských států k uplatňování této směrnice jsou v této oblasti důležité společné definice.

(8) Je třeba dosáhnout společného přístupu k základním prvkům trestných činů zavedením společných trestných činů neoprávněného přístupu k informačním systémům, neoprávněného zasahování do informačních systémů, neoprávněného zasahování do údajů a neoprávněného sledování.

(9) Sledování zahrnuje mimo jiné poslech, monitorování nebo kontrolu obsahu komunikace a získávání obsahu údajů, a to buď přímo přístupem a využitím informačních systémů, nebo nepřímo pomocí technických prostředků pro elektronický či jiný odposlech.

(10) Členské státy by měly stanovit sankce za útoky na informační systémy. Tyto sankce by měly být účinné, přiměřené a odrazující a jejich součástí by měl být trest odnětí svobody nebo peněžitý trest.

(11) Tato směrnice stanoví trestní sankce alespoň pro případy, které se nepovažují za méně závažné. Členské státy by měly mít možnost stanovit, co se rozumí méně závažným případem v souladu s jejich vnitrostátním právem a praxí. Za méně závažný případ lze považovat například situaci, kdy škoda vzniklá v důsledku trestného činu nebo ohrožení veřejných nebo soukromých zájmů nastalé v důsledku trestného činu, jako je například nedotknutelnost počítačového systému nebo počítačových údajů nebo nedotknutelnost osoby, jejích práv či jiných zájmů, jsou zanedbatelné nebo takové povahy, že uložení trestní sankce v rámci zákonné hranice trestních sazeb nebo uložení trestní odpovědnosti není nutné.

(12) Zjišťování a oznamování hrozeb a rizik vyplývajících z kybernetických útoků a zranitelnost informačních systémů s nimi související představují rozhodný faktor pro účinné předcházení kybernetickým útokům a reakci na ně a pro zdokonalování bezpečnosti informačních systémů. Poskytování pobídek k oznamování bezpečnostních nedostatků by mohlo přispět k tomuto zdokonalování. Členské státy by měly vynaložit úsilí k poskytnutí příležitostí pro zákonné odhalování a oznamování bezpečnostních nedostatků.

(13) Je vhodné zavést přísnější sankce v případě, že je útok na informační systém spáchán v rámci zločinného spolčení vymezeného v rámcovém rozhodnutí Rady 2008/841/SVV ze dne 24. října 2008 o boji proti organizované trestné činnosti [1], nebo pokud se jedná o rozsáhlý kybernetický útok, který má dopad na velký počet informačních systémů, včetně případu, kdy má útok vytvořit „botnet“, nebo pokud kybernetický útok způsobí závažnou škodu, včetně případu, kdy je útok proveden prostřednictvím „botnetu“. Je rovněž vhodné stanovit přísnější sankce, pokud je útok veden na kritickou infrastrukturu členského státu nebo Unie.

(14) Dalším důležitým prvkem integrovaného přístupu k boji proti kybernetické kriminalitě je zavedení účinných opatření proti krádeži totožnosti a jiným trestným činům týkajícím se totožnosti. Případnou akci na úrovni Unie proti tomuto druhu trestné činnosti by bylo možné zvážit také v rámci vyhodnocení potřeby existence komplexního horizontálního nástroje Unie.

(15) V závěrech ze zasedání Rady ve dnech 27. a 28. listopadu 2008 bylo uvedeno, že by se ve spolupráci s členskými státy a Komisí měla vypracovat nová strategie, která by přihlížela k obsahu Úmluvy Rady Evropy o kyberkriminalitě z roku 2001. Tato úmluva představuje právní referenční rámec pro boj s kybernetickou kriminalitou, včetně útoků na informační systémy. Tato směrnice z úmluvy vychází. Bezodkladné dokončení procesu ratifikace uvedené úmluvy ze strany všech členských států by proto mělo být považováno za prioritu.

(16) S ohledem na různé způsoby, jimiž lze útoky provést, a na rychlý vývoj hardwaru a softwaru odkazuje tato směrnice na nástroje, které lze používat k páchání trestných činů stanovených v této směrnici. Tyto nástroje by mohly zahrnovat škodlivý software, včetně softwaru schopného vytvářet botnety, používaný k páchání kybernetických útoků. I pokud je takový nástroj vhodný nebo obzvláště vhodný k páchání trestných činů stanovených v této směrnici, je možné, že byl vyroben pro zákonný účel. Je potřeba zabránit kriminalizaci v případech, kdy jsou tyto prostředky vyrobeny a uvedeny na trh pro zákonný účel, jako je testování spolehlivosti výrobků informačních technologií nebo bezpečnosti informačních systémů, a proto musí být kromě požadavku obecného úmyslu splněn také požadavek přímého úmyslu použít tyto prostředky pro účely spáchání některého z trestných činů stanovených v této směrnici.

(17) Cílem této směrnice není stanovit trestní odpovědnost v případech, kdy jsou naplněny znaky skutkové podstaty trestných činů stanovených v této směrnici, avšak tyto činy jsou spáchány bez protiprávního úmyslu, například pokud určitá osoba nevěděla, že se jedná o neoprávněný přístup, nebo v případě nařízeného testování či ochrany informačních systémů, například svěřila-li společnost či prodejce určité osobě úkol provést test odolnosti jejich bezpečnostního systému. V rámci této směrnice smluvní závazky nebo dohody o omezení přístupu k informačním systémům prostřednictvím uživatelské politiky nebo služebních podmínek, jakož i pracovněprávní spory ohledně přístupu k informačním systémům zaměstnavatele a jejich využívání k soukromým účelům by neměly vést ke vzniku trestní odpovědnosti v případech, kdy by přístup za těchto podmínek byl považován za neoprávněný, a představoval by tak jediný základ pro trestní řízení. Touto směrnicí není dotčeno právo na přístup k informacím, jak je stanoveno ve vnitrostátním právu a v právu Unie, toto právo však zároveň nesmí sloužit jako odůvodnění neoprávněného nebo svévolného přístupu k informacím.

[1] Úř. věst. L 300, 11.11.2008, s. 42.

(18) Kybernetické útoky by mohly být usnadněny různými okolnostmi, například pokud má pachatel v rámci svého zaměstnání přístup k bezpečnostním systémům spojeným se zasaženými informačními systémy. V rámci vnitrostátního práva by tyto okolnosti měly být v průběhu trestního řízení odpovídajícím způsobem zohledněny.

(19) Členské státy by ve svém vnitrostátním právu měly v souladu s příslušnými pravidly týkajícími se přitěžujících okolností danými jejich právním řádem stanovit přitěžující okolnosti. Měly by zajistit, aby soudci mohli k těmto přitěžujícím okolnostem přihlédnout při stanovení druhu trestu a jeho výměry pachateli. Je na uvážení soudce, aby tyto okolnosti posoudil spolu s ostatními skutečnostmi daného případu.

(20) Tato směrnice neupravuje, pokud jde o trestné činy v ní uvedené, podmínky pro provádění trestního stíhání, jako je oznámení oběti učiněné v místě, kde byl trestný čin spáchán, oznámení ze strany státu, na jehož území byl trestný čin spáchán, nebo nestíhání pachatele v místě, kde byl trestný čin spáchán.

(21) V rámci této směrnice musí státy a veřejnoprávní subjekty plně zajišťovat respektování lidských práv a základních svobod v souladu se stávajícími mezinárodními závazky.

(22) Tato směrnice posiluje význam sítí, jako je síť G8 nebo síť kontaktních míst Rady Evropy s nepřetržitým provozem. Tato kontaktní místa by měla být schopna poskytovat účinnou pomoc, a usnadňovat tak například výměnu příslušných dostupných informací poskytování technické pomoci či právních informací pro účely vyšetřování nebo soudních řízení ohledně trestných činů týkajících se informačních systémů a souvisejících údajů dožadujícího členského státu. Za účelem zajištění bezproblémového fungování sítí by mělo být každé kontaktní místo schopno urychleně komunikovat s kontaktním místem jiného členského státu za podpory mimo jiné vyškoleného a technicky vybaveného personálu. Vzhledem k rychlosti, kterou lze provést rozsáhlé kybernetické útoky, by členské státy měly mít možnost rychle reagovat na naléhavé žádosti z této sítě kontaktních míst. V těchto případech se může jevit účelné, aby žádost o informace obsahovala kontaktní telefonní číslo, díky němuž může dožadovaný členský stát zajistit, že žádost bude zpracována okamžitě a že do osmi hodin bude poskytnuta odpověď.

(23) Pro předcházení útokům na informační systémy a boj proti nim je velmi důležitá spolupráce veřejných orgánů na jedné straně a soukromého sektoru a občanské společnosti na straně druhé. Je nezbytné upevnit a zlepšit spolupráci mezi poskytovateli služeb, výrobci, donucovacími orgány a justičními orgány, a to při plném dodržování právních norem. Taková spolupráce by mohla zahrnovat podporu ze strany poskytovatelů služeb úsilí o zajištění potenciálních důkazů, při poskytování prvků přispívajících k identifikaci pachatelů a v krajním případě při úplném nebo částečném přerušení fungování informačních systémů nebo funkcí, jež byly ohroženy nebo zneužity pro protiprávní účely, provedeném v souladu s vnitrostátním právem a praxí. Členské státy by měly rovněž uvážit zřízení sítí pro spolupráci a partnerství, do nichž by byli zapojeni poskytovatelé služeb a výrobci za účelem výměny informací týkajících se trestných činů v oblasti působnosti této směrnice.

(24) Je třeba shromažďovat srovnatelné údaje o trestných činech stanovených v této směrnici. Pro získání ucelenější představy o problému kybernetické kriminality a o bezpečnosti sítí a informací na úrovni Unie a pro nalezení účinnějších forem reakce, by relevantní údaje měly být zpřístupněny příslušným specializovaným agenturám a institucím Unie, jako je Europol a agentura ENISA, v souladu s jejich úkoly a informačními potřebami. Členské státy by měly předávat informace o způsobu, jímž pachatelé páchají trestnou činnost, Europolu a jeho Evropskému centru pro boj proti kyberkriminalitě za účelem provedení posouzení hrozeb a strategických analýz kybernetické kriminality v souladu s rozhodnutím Rady 2009/371/SVV ze dne 6. dubna 2009 o zřízení Evropského policejního úřadu (Europol) ([1]). Poskytování informací může napomoci lepšímu porozumění stávajících budoucích hrozeb, a přispět tak k vhodnějšímu a cílenému rozhodování o boji proti útokům zaměřeným na informační systémy a k jejich předcházení.

(25) Komise by měla předložit zprávu o uplatňování této směrnice a připojit nezbytné legislativní návrhy, jež by mohly vést k rozšíření její oblasti působnosti, přičemž zohlední vývoj v oblasti kybernetické činnosti kriminality. Tento vývoj by mohl zahrnovat technologický vývoj, který například umožní účinnější prosazování práva v oblasti útoků na informační systémy či usnadní prevenci nebo zmírňování dopadů těchto útoků. Komise by za tímto účelem měla zohlednit dostupné analýzy a zprávy vypracované příslušnými aktéry a zejména Europolem a agenturou ENISA.

(26) Má-li být boj proti kybernetické kriminalitě účinný, je nutné zvýšit odolnost informačních systémů přijetím vhodných opatření s cílem účinněji je chránit před kybernetickými útoky. Členské státy by měly přijmout opatření nezbytná k ochraně své kritické infrastruktury před kybernetickými útoky, přičemž by v daném rámci měly zvážit ochranu svých informačních systémů a souvisejících údajů. Základní součástí komplexního přístupu účinnému boji proti kybernetické kriminalitě je zajištění

([1]) Úř. věst. L 121, 15.5.2009, s. 37.

odpovídající úrovně ochrany bezpečnosti informačních systémů právnickými osobami, například v souvislosti poskytováním veřejně dostupných služeb elektronických komunikací v souladu se stávajícími právními předpisy Unie v oblasti ochrany soukromí a elektronických komunikací a ochrany údajů. Je třeba poskytnout dostatečnou úroveň ochrany před přiměřeně rozpoznatelnými hrozbami a ochranu zranitelným místům v souladu se stavem techniky v konkrétním odvětví a s ohledem na konkrétní situaci zpracování údajů. Náklady a zátěž vzniklé v souvislosti s touto ochranou by měly odpovídat pravděpodobné výši škody, která by dotčeným subjektům v důsledku kybernetického útoku vznikla. Členské státy se vybízí, aby pro případy, kdy právnická osoba jednoznačně nezajistila odpovídající úroveň ochrany proti kybernetickým útokům, stanovily příslušná opatření k zajištění odpovědnosti podle jejich vnitrostátního práva.

(27) Výrazné nedostatky a rozdíly v právu a v trestních řízeních členských států v oblasti útoků na informační systémy mohou bránit boji s organizovanou trestnou činností a terorismem a mohou komplikovat efektivní policejní a justiční spolupráci v této oblasti. Z nadnárodní hranicemi neomezené povahy moderních informačních systémů vyplývá, že útoky na tyto systémy mají přeshraniční rozměr, což podtrhuje naléhavou potřebu dalších opatření na sbližování ustanovení trestního práva v této oblasti. Kromě toho by koordinace stíhání případů útoků na informační systémy měla být usnadněna odpovídajícím prováděním uplatňováním rámcového rozhodnutí Rady 2009/948/SVV ze dne 30. listopadu 2009 předcházení kompetenčním sporům při výkonu pravomoci v trestním řízení a jejich řešení ([1]). Členské státy by ve spolupráci s Unií měly také usilovat o zlepšení mezinárodní spolupráce týkající se bezpečnosti informačních systémů, počítačových sítí a počítačových údajů. V případě jakékoli mezinárodní dohody zahrnující výměnu údajů by měla být věnována řádná pozornost bezpečnosti předávání a uchovávání údajů.

(28) Lepší spolupráce mezi příslušnými donucovacími orgány a justičními orgány v celé Unii je pro efektivitu boje proti kybernetické kriminalitě nezbytná. V této souvislosti je třeba podpořit zvýšení úsilí s cílem poskytnout příslušným orgánům odpovídající odbornou přípravu v zájmu většího povědomí o kybernetické kriminalitě a jejím dopadu a posílit spolupráci a výměnu osvědčených postupů, například prostřednictvím příslušných specializovaných agentur a institucí Unie. Tato odborná příprava by měla být mimo jiné zaměřena na zvyšování povědomí o odlišnostech jednotlivých vnitrostátních právních řádů, možných právních a technických výzvách v rámci vyšetřování v trestních věcech a o rozdělení pravomocí mezi příslušné vnitrostátní orgány.

(29) Tato směrnice respektuje lidská práv a základní svobody a ctí zásady uznané zejména Listinou základních práv Evropské unie a Evropskou úmluvou o ochraně lidských práv a základních svobod, včetně ochrany osobních údajů, práva na soukromí, svobody projevu a informací, práva na spravedlivý proces, presumpce neviny a práva na obhajobu i zásady zákonnosti a přiměřenosti trestných činů a trestů. Cílem této směrnice je zejména zajistit plné dodržování těchto práv a zásad a v souladu s nimi musí být provedena.

(30) Ochrana osobních údajů je jedním ze základních práv podle čl. 16 odst. 1 Smlouvy o fungování Evropské unie a článku 8 Listiny základních práv Evropské unie. Veškeré zpracovávání osobních údajů v souvislosti s prováděním této směrnice by proto mělo být plně v souladu s příslušnými právními předpisy Unie v oblasti ochrany údajů.

(31) V souladu s článkem 3 Protokolu o postavení Spojeného království a Irska s ohledem na prostor svobody, bezpečnosti a práva, připojeného ke Smlouvě o Evropské unii a ke Smlouvě o fungování Evropské unie, oznámily tyto členské státy své přání účastnit se přijímání a používání této směrnice.

(32) V souladu s články 1 a 2 Protokolu o postavení Dánska, připojeného ke Smlouvě o Evropské unii a ke Smlouvě o fungování Evropské unie, se Dánsko neúčastní přijímání této směrnice, a tato směrnice pro ně není závazná ani použitelná.

(33) Jelikož cílů této směrnice, totiž zajistit, aby se na útoky na informační systémy ve všech členských státech vztahovaly účinné, přiměřené a odrazující trestní sankce, a zlepšit a podpořit spolupráci mezi justičními a jinými příslušnými orgány, nemůže být uspokojivě dosaženo na úrovni členských států, a proto jich může být z důvodu jejich rozsahu účinků, lépe dosaženo na úrovni Unie, může Unie přijmout opatření v souladu se zásadou subsidiarity stanovenou v článku 5 Smlouvy o Evropské unii. V souladu se zásadou proporcionality stanovenou v uvedeném článku nepřekračuje tato směrnice rámec toho, co je nezbytné pro dosažení těchto cílů.

(34) Cílem této směrnice je pozměnit a rozšířit působnost ustanovení rámcového rozhodnutí Rady 2005/222/SVV ze dne 24. února 2005 o útocích proti informačním systémům ([2]). Vzhledem k tomu, že změn, které je třeba provést, je značný počet a jsou podstatné, mělo by být rámcové rozhodnutí 2005/222/SVV v zájmu přehlednosti nahrazeno v plném rozsahu ve vztahu k členským státům, které se účastní přijímání této směrnice,

([1]) Úř. věst. L 328, 15.12.2009, s. 42.

([2]) Úř. věst. L 69, 16.3.2005, s. 67.

PŘIJALY TUTO SMĚRNICI:

Článek 1

Předmět

Tato směrnice stanoví minimální pravidla týkající se vymezení trestných činů a sankcí ve vztahu k útokům na informační systémy. Jejím cílem je rovněž usnadnit předcházení těmto trestným činům a zlepšit spolupráci mezi justičními a jinými příslušnými orgány.

Článek 2

Definice

Pro účely této směrnice se rozumí:

a) „informačním systémem" jakýkoli přístroj nebo skupina vzájemně propojených nebo přidružených přístrojů, z nichž jeden nebo více provádí na základě programu automatické zpracování počítačových údajů, jakož i počítačové údaje uložené, zpracované, opětovně vyhledané nebo přenesené tímto přístrojem či skupinou přístrojů za účelem jeho či jejich provozu, použití, ochrany a údržby;

b) „počítačovými údaji" jakékoli zachycení skutečností, informací nebo pojmů ve formě vhodné ke zpracování informačním systémem, včetně programu vhodného k zajištění provedení některé funkce informačním systémem;

c) „právnickou osobou" každý subjekt, který má postavení právnické osoby podle příslušného práva, avšak nejedná se o státy, nebo veřejnoprávní subjekty při výkonu veřejné moci nebo organizace mezinárodního práva veřejného;

d) „neoprávněným" jednání uvedené v této směrnici včetně přístupu, zásahu nebo sledování, které není povoleno majitelem či jiným držitelem práv k systému nebo k jeho části nebo které není povoleno vnitrostátním právem.

Článek 3

Neoprávněný přístup k informačním systémům

Členské státy přijmou nezbytná opatření k zajištění toho, aby neoprávněný přístup k celému informačnímu systému nebo k některé jeho části je-li spáchán úmyslně, byl trestným činem, je-li tím porušeno bezpečnostního opatření, a to alespoň tehdy, pokud se nejedná o méně závažný případ.

Článek 4

Neoprávněné zasahování do informačních systémů

Členské státy přijmou nezbytná opatření k zajištění toho, aby úmyslné a neoprávněné závažné narušení nebo přerušení fungování informačního systému vložením počítačových údajů či jejich přenosem, poškozením, vymazáním, znehodnocením, pozměněním, potlačením nebo znepřístupněním bylo trestným činem, a to alespoň tehdy, pokud se nejedná o méně závažný případ.

Článek 5

Neoprávněné zasahování do údajů

Členské státy přijmou nezbytná opatření k zajištění toho, aby úmyslné a neoprávněné vymazání, poškození, znehodnocení, pozměnění nebo potlačení počítačových údajů v informačním systému, nebo jejich znepřístupnění bylo trestným činem, a to alespoň tehdy, pokud se nejedná o méně závažný případ.

Článek 6

Neoprávněné sledování údajů

Členské státy přijmou nezbytná opatření k zajištění toho, aby úmyslné a neoprávněné sledování neveřejných přenosů počítačových údajů do, z nebo uvnitř informačního systému prováděné technickými prostředky, včetně elektromagnetického záření z informačního systému nesoucího takové počítačové údaje, bylo trestným činem, a to alespoň tehdy, pokud se nejedná o méně závažný případ.

Článek 7

Nástroje použité k páchání trestných činů

Členské státy přijmou nezbytná opatření k zajištění toho, aby úmyslná výroba, prodej, opatření si k užití, dovoz, distribuce nebo jiné formy zpřístupnění některého z následujících nástrojů byly trestným činem, jsou-li provedeny neoprávněně a se záměrem použít tyto nástroje pro účely spáchání některého z trestných činů uvedených v článcích 3 až 6, a to alespoň tehdy, pokud se nejedná o méně závažný případ:

a) počítačového programu, který byl vytvořen nebo přizpůsoben prvotně pro účely spáchání některého z trestných činů uvedených v článcích 3 až 6;

b) počítačového hesla, přístupového kódu nebo obdobných údajů, které umožňují přístup k celému informačnímu systému nebo k jeho části.

Článek 8

Návod, pomoc nebo jiná forma účastenství a pokus

1. Členské státy zajistí trestnost návodu, pomoci či jiné formy účastenství na spáchání trestných činů uvedených v článcích 3 až 7.

2. Členské státy zajistí trestnost pokusu trestných činů uvedených v článcích 4 až 5.

Článek 9

Sankce

1. Členské státy přijmou opatření nezbytná k zajištění toho, aby pro trestné činy uvedené v článcích 3 až 8 byly stanoveny účinné, přiměřené a odrazující trestní sankce.

2. Členské státy přijmou opatření nezbytná k zajištění toho, aby pro trestné činy uvedené v článcích 3 až 7 byl stanoven trest odnětí svobody s horní hranicí trestní sazby nejméně dva roky, a to alespoň tehdy, pokud se nejedná o méně závažný případ.

3. Členské státy přijmou opatření nezbytná k zajištění toho, aby byl pro trestné činy uvedené v článcích 4 a 5 stanoven trest odnětí svobody s horní hranicí trestní sazby nejméně tři roky, jsou-li spáchány úmyslně a pokud došlo k útoku s dopadem na

velký počet informačních systémů za použití nástroje uvedeného v článku 7, vytvořeného nebo přizpůsobeného prvotně pro tento účel.

4. Členské státy přijmou opatření nezbytná k zajištění toho, aby pro trestné činy uvedené v článcích 4 a 5 byl stanoven trest odnětí svobody s horní hranicí trestní sazby nejméně pět let, pokud:

a) byly spáchány v rámci zločinného spolčení vymezeného v rámcovém rozhodnutí Rady 2008/841/SVV bez ohledu na trestní sazbu stanovenou v uvedeném rozhodnutí;

b) jejich spácháním byla způsobena závažná škoda, nebo

c) byly spáchány proti informačnímu systému kritické infrastruktury.

5. Členské státy přijmou opatření nezbytná k zajištění toho, aby v případě, že trestné činy uvedené v článcích 4 a 5 byly spáchány prostřednictvím zneužití osobních údajů jiné osoby s cílem získat důvěru třetí strany, čímž vznikla újma skutečnému nositeli totožnosti, mohla být tato skutečnost v souladu s vnitrostátním právem považována za přitěžující okolnost, není-li takováto okolnost již zahrnuta ve skutkové podstatě jiného činu, který je podle vnitrostátního práva trestný.

Článek 10

Odpovědnost právnických osob

1. Členské státy přijmou opatření nezbytná k zajištění toho, aby právnické osoby mohly být činěny odpovědnými za trestné činy uvedené v článcích 3 až 8, spáchané v jejich prospěch osobou jednající samostatně nebo jako člen orgánu dané právnické osoby, která v rámci této právnické osoby působí ve vedoucím postavení na základě oprávnění:

a) jednat jménem této právnické osoby;

b) přijímat rozhodnutí jménem této právnické osoby;

c) vykonávat kontrolu v rámci této právnické osoby.

2. Členské státy přijmou opatření nezbytná k zajištění toho, aby právnické osoby mohly být činěny odpovědnými v případech, kdy nedostatek dohledu nebo kontroly ze strany osoby uvedené v odstavci 1 umožnil spáchání trestných činů uvedených v článcích 3 až 8 ve prospěch této právnické osoby osobou jí podřízenou.

3. Odpovědnost právnických osob podle odstavců 1 a 2 nevylučuje trestní stíhání fyzických osob, které jsou pachateli, návodci, pomocníky či podílníky trestných činů uvedených v článcích 3 až 8.

Článek 11

Sankce vůči právnickým osobám

1. Členské státy přijmou opatření nezbytná k zajištění toho, aby právnické osoby odpovědné podle čl. 10 odst. 1 podléhaly účinným, přiměřeným a odrazujícím sankcím, které zahrnují pokuty trestní nebo jiné povahy, a které mohou zahrnovat i jiné sankce, jako například:

a) zbavení oprávnění pobírat veřejné výhody nebo podpory;

b) dočasný nebo trvalý zákaz provozování obchodní činnosti;

c) uložení soudního dohledu;

d) zrušení této právnické osoby rozhodnutím soudu;

e) dočasné nebo trvalé uzavření provozoven použitých ke spáchání trestného činu.

2. Členské státy přijmou opatření nezbytná k zajištění toho, aby právnické osoby odpovědné podle čl. 10 odst. 2 podléhaly účinným, přiměřeným a odrazujícím sankcím nebo jiným opatřením.

Článek 12

Soudní příslušnost

1. Členské státy stanoví svou soudní příslušnost ve vztahu k trestným činům uvedeným v článcích 3 až 8, které byly spáchány:

a) zcela nebo částečně na jejich území nebo

b) jejich státními příslušníky, alespoň v případech, kdy je daný skutek trestným činem v místě, kde byl spáchán.

2. Při stanovení své soudní příslušnosti podle odst. 1 písm. a) členský stát zajistí, aby tato příslušnost zahrnovala případy, kdy:

a) pachatel spáchal trestný čin v době své fyzické přítomnosti na jeho území, a to bez ohledu na to, zda byl trestný čin namířen proti informačnímu systému na jeho území či nikoli, nebo

b) trestný čin byl namířen proti informačnímu systému na jeho území, a to bez ohledu na to, zda pachatel spáchal trestný čin v době své fyzické přítomnosti na jeho území či nikoli.

3. Členský stát informuje Komisi, pokud se rozhodne rozšířit soudní příslušnost ve vztahu k trestným činům uvedeným v článcích 3 až 8, které byly spáchány mimo jeho území, mimo jiné pokud:

a) má pachatel obvyklé bydliště na jeho území nebo

b) je trestný čin spáchán ve prospěch právnické osoby usazené na jeho území.

Článek 13

Výměna informací

1. Za účelem výměny informací týkajících se trestných činů uvedených v článcích 3 až 8 členské státy zajistí, aby měly k dispozici funkční národní kontaktní místo, a aby využívaly stávající síť funkčních kontaktních míst s nepřetržitým provozem. Členské státy rovněž zajistí, aby byly zavedeny postupy, které příslušnému orgánu v případě naléhavých žádostí o pomoc umožní podat nejpozději osm hodin od obdržení žádosti informaci alespoň o tom, zda bude na žádost o pomoc reagovat, a dále uvést formu a předpokládaný termín této reakce.

2. Členské státy informují Komisi o kontaktních místech uvedených v odstavci 1, která určily. Komise tyto informace předá ostatním členským státům a příslušným specializovaným agenturám a institucím Unie.

3. Členské státy přijmou opatření nezbytná k zajištění toho, aby měly za účelem usnadnění neprodleného oznamování trestných činů uvedených v článcích 3 až 6 příslušné vnitrostátní orgány k dispozici vhodné informační kanály.

Článek 14

Sledování a statistika

1. Členské státy zajistí, aby byl zaveden systém pro záznam, produkci a poskytování statistických údajů o trestných činech uvedených v článcích 3 až 7.

2. Statistické údaje uvedené v odstavci 1 musí zahrnovat alespoň stávající údaje o počtu trestných činů uvedených v článcích 3 až 7 zaznamenaných členskými státy a o počtu osob stíhaných a odsouzených za spáchání trestných činů uvedených v článcích 3 až 7.

3. Údaje shromážděné podle tohoto článku předávají členské státy Komisi. Komise zajistí, že komplexní přehled těchto statistických zpráv bude zveřejněn a předložen příslušným specializovaným agenturám a institucím Unie.

Článek 15

Nahrazení rámcového rozhodnutí 2005/222/SVV

Rámcové rozhodnutí 2005/222/SVV se nahrazuje ve vztahu k členským státům, které se účastní přijímání této směrnice, aniž jsou dotčeny povinnosti členských států týkající se lhůt pro provedení rámcového rozhodnutí ve vnitrostátním právu.

Ve vztahu k členským státům, které se účastní přijímání této směrnice, se odkazy na rámcové rozhodnutí 2005/222/SVV považují za odkazy na tuto směrnici.

Článek 16

Provedení

1. Členské státy uvedou v účinnost právní a správní předpisy nezbytné pro dosažení souladu s touto směrnicí do 4. září 2015.

2. Členské státy předloží Komisi znění vnitrostátních právních předpisů, kterými ve svém vnitrostátním právu provádějí povinnosti, jež pro ně vyplývají z této směrnice.

3. Tyto předpisy přijaté členskými státy musí obsahovat odkaz na tuto směrnici nebo musí být takový odkaz učiněn při jejich úředním vyhlášení. Způsob odkazu si stanoví členské státy.

Článek 17

Podávání zpráv

Do 4. září 2017 předloží Komise Evropskému parlamentu a Radě zprávu, ve které zhodnotí, do jaké míry členské státy přijaly opatření nezbytná k dosažení souladu s touto směrnicí, a případně připojí legislativní návrhy. Komise v této souvislosti rovněž zohlední technický a právní vývoj v oblasti kybernetické kriminality, a to zejména s ohledem na oblast působnosti této směrnice.

Článek 18

Vstup v platnost

Tato směrnice vstupuje v platnost dvacátým dnem po vyhlášení v *Úředním věstníku Evropské unie*.

Článek 19

Určení

Tato směrnice je určena členským státům v souladu se Smlouvami.

V Bruselu dne 12. srpna 2013.

Za Evropský parlament	*Za Radu*
předseda	*předseda*
M. SCHULZ	L. LINKEVIČIUS