BACKGROUND REPORT

PRAGUE**PRAŽSKÝ**
STUDENT**STUDENTSKÝ**
SUMMIT

EU

Kybernetická bezpečnost

1. Úvod

Internet se v posledních dvou desetiletích stal nedílnou součástí společnosti. Otevřený a svobodný kyberprostor odstranil bariéry mezi zeměmi a jejich občany, umožnil celosvětovou interakci a sdílení myšlenek a poskytl fórum pro svobodu projevu a výkon základních práv.

Náš každodenní život, sociální interakce i ekonomika jsou do značné míry spjaty s dokonalým fungováním informačních a komunikačních technologií. Ty se staly páteří ekonomického růstu a zdrojem, na němž závisí všechna hospodářská odvětví. Jsou základem komplexních systémů, jež udržují světovou ekonomiku v chodu v klíčových odvětvích, jako jsou například finanční služby, energetika, zdravotnictví či doprava.

Prosperita společnosti bude na internetu záviset stále větší měrou. Je nutné, aby internet zůstal svobodný a inovativní, a aby soukromý sektor a občanská společnost nadále přispívaly k jeho rozvoji a růstu. Svoboda na internetu si však také žádá jeho bezpečnost a ochranu. Digitální svět nepopiratelně přináší obrovské výhody, ale nesmí se zapomínat na jeho zranitelnost. Incidenty v oblasti kybernetické bezpečnosti se v posledních letech množí znepokojivou rychlostí. Hrozby mohou mít různý původ, od kriminálních či teroristických útoků až po přírodní katastrofy či neúmyslné chyby. Pachatelé kyberkriminality navíc používají stále rafinovanější metody, jak do informačních systémů proniknout.[1]

Výše uvedené důvody vedly Evropskou unii k zintenzivnění své činnosti v této oblasti. V únoru tohoto roku předložila Komise společně s vysokou představitelkou Unie pro zahraniční věci a bezpečnostní politiku Catherine Ashtonovou návrh strategie kybernetické bezpečnosti Evropské unie „Otevřený, bezpečný a chráněný kyberprostor". Představuje zde vizi EU o tom, jak co nejlépe předcházet počítačovým útokům a jak na ně reagovat. Cílem je posílit evropské hodnoty svobody a demokracie a zajistit bezpečný růst digitální ekonomiky.

Strategie je rozdělena do pěti základních priorit, jež řeší výše uvedené problémy:

- Dosažení kybernetické odolnosti
- Výrazné omezení kyberkriminality
- Rozvoj politiky a kapacit kybernetické obrany v souvislosti se společnou bezpečnostní a obrannou politikou (SBOP)
- Rozvoj průmyslových a technologických zdrojů pro kybernetickou bezpečnost
- Zavedení soudržné mezinárodní politiky Evropské unie týkající se kyberprostoru a podpora základních hodnot EU

Catherine Ashtonová k tomu uvedla: *„Aby zůstal kybernetický prostor otevřený a svobodný, měly by „online" fungovat tytéž normy, zásady a hodnoty, které EU podporuje „offline". Základní práva, demokracie a zásady právního státu je třeba chránit i v kybernetickém*

[1] Strategie kybernetické bezpečnosti EU: Otevřený, bezpečný a chráněný kyberprostor. *Evropská komise*. [online]. ©2013. Dostupné z: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=JOIN:2013:0001:FIN:CS:PDF.

prostoru. Na celosvětové podpoře těchto práv spolupracuje EU se svými mezinárodními partnery, jakož i s občanskou společností a soukromým sektorem."[2]

Předmětem našeho bližšího zájmu však bude dále pouze návrh směrnice o zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii (návrh zde), která představuje hlavní prvek celkové strategie. Tento návrh směrnice bude jedním z bodů agendy, o které se bude jednat na konferenci.

2. Co směrnice navrhuje

2.1 Národní rámec pro bezpečnost sítí a informací

Každý členský stát přijme národní strategii, která vymezí strategické cíle a zákonná opatření k dosažení a udržení vysoké úrovně bezpečnosti sítí a informací. Cíle a priority by měly být stanoveny na základě aktuální analýzy rizik a incidentů. Strategie by měla vytvořit rámec pro naplněný těchto cílů, včetně jasného vymezení pravomocí a odpovědnosti jednotlivých vládních orgánů a jiných relevantních subjektů. Měla by obsahovat obecná opatření týkající se připravenosti a reakce na kybernetické hrozby. Vedle toho by měla zahrnovat i určení vzdělávacích a školících programů, jakož i plány výzkumu a vývoje v oblasti kybernetické bezpečnosti.

Součástí národní strategie bude dále národní plán pro bezpečnost sítí a informací. Ten by měl obsahovat plán pro posouzení rizik a posouzení dopadů možných incidentů. Všechny strany zapojené do realizace plánu musí mít vymezeny pravomoci a odpovědnost a plán by měl rovněž určit postupy jejich spolupráce a komunikace při zajišťování prevence, reakce a nápravy. Jak národní strategie, tak národní plán by musely být sděleny Komisi do jednoho měsíce od přijetí směrnice.

Směrnice dále stanovuje povinnost členského státu jmenovat národní orgán odpovědný za bezpečnost sítí a informačních systémů (dále jen „odpovědný orgán"). Ten bude vykonávat dohled nad uplatňováním této směrnice na vnitrostátní úrovni a přispívat k jejímu jednotnému uplatňování na úrovni Unie. Členský stát musí národnímu orgánu poskytnout odpovídající technické, finanční a lidské zdroje k plnění tohoto úkolu.

Členský stát také musí zřídit skupinu pro reakci na počítačové hrozby (CERT), jež bude odpovědná za řešení incidentů a rizik. Rovněž CERT musí mít zajištěné odpovídající zdroje nezbytné pro účinné plnění svěřených úkolů. CERT bude podřízena odpovědnému orgánu, který bude pravidelně přezkoumávat účinnost postupu při řešení incidentů.

2.2 Spolupráce mezi odpovědnými orgány

Odpovědné orgány jednotlivých členských států a Komise zřídí síť na ochranu proti rizikům a incidentům narušujícím bezpečnost sítí a informačních systémů. Tato síť bude představovat stále komunikační spojení mezi odpovědnými orgány a Komisí. Do sítě bude

[2] Plán počítačové bezpečnosti v EU má chránit otevřený internet a svobodu a příležitosti v on-line prostředí. *Evropská komise.* [online]. ©2013. [cit. 2013-03-04]. Dostupné z: http://ec.europa.eu/ceskarepublika/press/press_releases/13_94_cs.htm.

navíc zapojena již existující Evropská agentura pro bezpečnost sítí a informací (ENISA), která na žádost poskytne síti své odborné znalosti a doporučení.

Odpovědné orgány budou prostřednictvím sítě pro spolupráci vydávat včasná varování ohledně rizik a incidentů, jejichž rozsah rychle roste nebo které překračují národní reakční kapacitu či postihují více než jeden členský stát (postačuje splnění alespoň jedné z těchto podmínek). V rámci včasného varování budou odpovědné orgány nebo Komise sdělovat veškeré relevantní informace, které mají k dispozici a které by mohly být užitečné při posuzování daného rizika či incidentu. Pokud navíc panuje podezření, že daný incident má povahu trestného činu, uvědomí odpovědné orgány či Komise Evropské centrum pro boj proti kriminalitě (toto centrum již existuje a spadá pod Europol). Po vydání včasného varování odpovědné orgány posoudí relevantní informace a následně se dohodnou na koordinované reakci.

Formy a postupy, kterými budou odpovědné orgány sdělovat síti pro spolupráci relevantní informace, jakož i kritéria pro posouzení rizik v rámci sítě stanoví unijní plán spolupráce v oblasti bezpečnosti sítí a informací, k jehož přijetí je prostřednictvím prováděcích aktů zmocněna Komise. Tento plán bude rovněž obsahovat postupy pro následnou koordinovanou reakci, včetně určení pravomocí a odpovědnosti jednotlivých orgánů.

V rámci sítě pro spolupráci mohou dále odpovědné orgány a Komise projednávat a posuzovat národní strategie a národní plány a účinnost skupin CERT. Síť bude dále sloužit jako fórum pro výměnu informací a osvědčených postupů mezi odpovědnými orgány a rovněž napomáhat jejich vzájemné součinnosti při budování kapacit pro bezpečnost sítí a informací.

Výměna citlivých a důvěrných informací uvnitř této sítě bude probíhat s pomocí bezpečné infrastruktury. Aby byly členské státy oprávněny používat tento bezpečný systém, budou muset splňovat určitá technická, finanční a personální kritéria, k jejichž formulaci je zmocněna Komise.

2.3 Bezpečnost sítí a informačních systémů orgánů veřejné správy a hospodářských subjektů

Členské státy musí zajistit, aby jejich orgány veřejné správy a hospodářské subjekty přijaly vhodná technická a organizační opatření k řízení bezpečnostních rizik, jimž čelí jimi kontrolované a používané sítě a informační systémy. S ohledem na současné technické možnosti musí tato opatření zajišťovat takovou úroveň bezpečnosti, která odpovídá míře existujícího rizika. Zejména budou přijata taková opatření, která zabrání vzniku bezpečnostních incidentů v jejich sítích a informačních systémech, jež by poškodily jimi poskytované základní služby, případně minimalizují dopad takových incidentů, a zajistí tak kontinuitu služeb podporovaných těmito sítěmi a informačními systémy.

Vedle toho mají orgány veřejné správy a hospodářské subjekty povinnost oznamovat odpovědným orgánům incidenty, které mají významný dopad na bezpečnost jimi poskytovaných základních služeb. K určení okolností, za nichž jsou tyto subjekty povinny incident oznámit, je opět zmocněna Komise. Pokud navíc odpovědný orgán rozhodne, že je

ve veřejném zájmu, aby byl daný incident zveřejněn, je oprávněn o něm informovat veřejnost.

Tyto povinnosti, tedy přijetí opatření k řízení rizik a oznamovací povinnost, platí pro všechny hospodářské subjekty poskytující služby v Evropské unii. Hospodářský subjekt je pro účely této směrnice definován jako poskytovatel služeb informační společnosti, na nichž závisí poskytování dalších služeb informační společnosti (platformy pro elektronické obchodování, internetové platební brány, sociální sítě, vyhledávače, služby cloud computingu, obchody s aplikacemi atd.) nebo provozovatel kritické infrastruktury, která má zásadní význam pro poskytování důležitých ekonomických a společenských činností v oblasti energetiky, dopravy, bankovnictví, obchodování s cennými papíry a zdravotnictví.

Odpovědné orgány budou disponovat všemi nezbytnými pravomocemi pro vyšetřování porušení těchto povinností ze strany orgánů veřejné správy a hospodářských subjektů. Navíc budou oprávněny požadovat od nich informace potřebné k posouzení bezpečnosti jejich sítí a informačních systémů, podrobovat je bezpečnostním auditům, které bude provádět nezávislý orgán, a dávat jim závazné pokyny, jež budou soudně přezkoumatelné.

2.4 Závěrečná ustanovení

Členské státy si samy stanoví pravidla pro sankce za porušení vnitrostátních právních norem přijatých na základě této směrnice. Ty by měly být účinné, přiměřené a odrazující. Vnitrostátní právní a správní předpisy nezbytné pro dosažení souladu s touto směrnicí pak musí členské státy přijmout nejpozději do jednoho a půl roku po přijetí směrnice.

3. Důvody Komise pro vznik směrnice

Informační systémy jsou stále důležitější pro ekonomiku i společnost. Jejich bezpečnost však může narušit lidská chyba, přírodní katastrofa, technické selhání či úmyslný útok. Jejich selhání pak může bránit ve výkonu hospodářské činnosti, způsobit značné finanční ztráty a nepříznivě ovlivnit fungování společnosti.

Digitální informační systémy jsou vzájemně propojené napříč členskými státy a hrají důležitou roli při pohybu přeshraničního pohybu zboží, služeb a osob. Jejich stabilita je tedy nezbytným předpokladem pro hladké fungování vnitřního trhu. Zvýšená četnost výskytu bezpečnostních incidentů navíc podrývá důvěru veřejnosti v tyto informační systémy a znemožňuje tak plné rozvinutí digitálního trhu. Například průzkum Eurobarometru o kybernetické bezpečnosti z roku 2012 zjistil, že 38% uživatelů internetu v EU se obává, že online platby nejsou bezpečné, a kvůli tomu změnili své chování – 18% z nich si z těchto důvodů nebude kupovat žádné zboží online a 15% nebude využívat internetové bankovnictví.[3]

Dosavadní přístup v EU je založen čistě na dobrovolné bázi. Úroveň kapacit a připravenosti v jednotlivých členských státech se velmi liší a panuje roztříštěnost různých přístupu. Důsledkem je různá úroveň ochrany spotřebitelů a podniků a zhoršená celková

[3] Special Eurobarometer 390. *European commission.* [online]. ©2012. [cit. 2013-03-04]. Dostupné z: http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf.

úroveň ochrany v Unii. Narušení informačního systému v jednom členském státě se totiž může dotknout i jiných členských států a Unie jako celku. Neexistence efektivní spolupráce způsobuje nekoordinované regulatorní zásahy, nesourodé strategie a rozdílné standardy v jednotlivých členských státech. Mohou tak vznikat překážky na vnitřním trhu a spolu s nimi náklady na dodržování rozdílných předpisů pro firmy působící ve více členských státech.

Údaje o současné kybernetické bezpečnosti:

- Odhaduje se, že se denně vyskytne 150 000 počítačových virů a je napadeno 148 000 počítačů
- Podle Světového ekonomického fóra existuje 10% pravděpodobnost, že v nadcházejícím desetiletí dojde ke kolapsu významné kritické informační infrastruktury, což by mohlo způsobit škody ve výši přibližně 250 miliard USD.
- Příčinou velké části událostí ohrožujících bezpečnost sítí je počítačová trestná činnost. Společnost Symantec odhaduje, že oběti počítačové trestné činnosti přicházejí každoročně o přibližně 290 miliard EUR, a studie společnosti McAfee odhaduje roční zisky pachatelů počítačové trestné činnosti na 750 miliard EUR.
- Z veřejné konzultace o bezpečnosti sítí a informací vyplynulo, že 56,8 % respondentů zaznamenalo během uplynulého roku bezpečnostní události, které měly závažný dopad na jejich činnost.
- Podle Eurostatu mělo do ledna 2012 v EU formálně vymezenou bezpečnostní politiku v oblasti informačních a komunikačních technologií pouze 26 % podniků.[4]

4. Otázky spojené s návrhem směrnice

Je Komise oprávněna vydat tuto směrnici?

Podle čl. 14 Smlouvy o fungování EU může Unie přijímat „opatření ke sbližování právních a správních předpisů členských států, jejichž účelem je vytvoření a fungování vnitřního trhu". Jak již bylo uvedeno výše, Komise spatřuje v zajištění spolehlivého fungování informačních systémů zásadní předpoklad pro výkon příhraničního pohybu zboží, služeb a osob. Internet je ze své podstaty globálním nástrojem a vzhledem k propojenosti tak může narušení systému v jednom členském státu ohrozit další členské státy i Unii jako celek. Komise tak zaujala stanovisko, že v zájmu rozvoje vnitřního trhu je nutné předpisy týkající se bezpečnosti sítí a informací sladit.

Splňuje návrh Komise zásadu subsidiarity a proporcionality?

Dle Komise by absence zásahu ze strany EU vzhledem k přeshraniční povaze bezpečnosti sítí a informací znamenala, že jednotlivé členské státy budou jednat samostatně, a nebude tak možné dosáhnout patřičné koordinace potřebné k řízení rizik na příhraniční úrovni. Přístup založený na dobrovolnosti vedl k tomu, že spolu spolupracuje pouze úzká skupina členských států, které mají kapacity na vysoké úrovni. Aby se mohly do spolupráce zapojit všechny členské státy, musí být zajištěna minimální úroveň každého z nich. Dle

[4] Plán počítačové bezpečnosti v EU má chránit otevřený internet a svobodu a příležitosti v on-line prostředí. *Evropská komise.* [online]. ©2013. [cit. 2013-03-04]. Dostupné z: http://ec.europa.eu/ceskarepublika/press/press_releases/13_94_cs.htm .

Komise tak bude požadovaných cílů snáze dosáhnuto na úrovni Unie než na úrovni jednotlivých členských států.

Komise tvrdí, že návrh směrnice splňuje i zásadu proporcionality, neboť povinnosti členských států jsou nastaveny na nejnižší možné úrovni nezbytné k zajištění koordinované spolupráce. Z povahy směrnice pak vyplývá, že členské státy budou moci při provádění směrnice zohlednit svá vnitrostátní specifika. Každý členský stát také může směrnici provádět s ohledem na skutečná rizika, kterým čelí a jež uvedl ve své národní strategii.

Kterých hospodářských subjektů by se směrnice týkala?

Hospodářským subjektem je míněn poskytovatel služeb informační společnosti či provozovatel kritické infrastruktury (demonstrativní výčet subjektů, které spadají do těchto kategorií, byl uveden výše). Vývojáři softwaru nebo hardwaru jsou z této směrnice vyňaty. Důležité je zmínit, že směrnice se týká všech těchto subjektů, kteří provozují svou činnost na území EU. To tedy znamená, že uvedené povinnosti budou spadat i na společnosti, které nemají svoji centrálu v Unii. To by například byla významná změna pro společnosti z USA, protože ty mají v současné době velký prostor pro uvážení, které incidenty považují za významné a hodné zveřejnění (povinnost mají pouze v případě, když panuje podezření, že útočníci získali informace o zákaznících). Směrnice se navíc týká širšího spektra subjektů, například sociální sítě či obchody s aplikacemi nejsou v USA, na rozdíl od návrhu této směrnice, považovány za kritickou infrastrukturu.[5] Kybernetická politika Spojených států se vydává podobný směrem, jaký navrhuje směrnice, ovšem na rozdíl od ní je ve větší míře založená na dobrovolnosti (více zde).

Nebude povinnost zavedení systému pro řízení rizik a oznamovací povinnost pro hospodářské subjekty znamenat nepřiměřené náklady?

Komise argumentuje tím, že tyto povinnosti se vztahují pouze na klíčové subjekty a vyžaduje opatření úměrná daným rizikům. Řadě subjektů coby správců údajů ukládá povinnost zajistit ochranu osobních údajů již současná legislativa. Dle Komise tak nedojde k přetížení malých a středních podniků, neboť jejich povinnosti budou přiměřené rizikům, jež dotčené sítě a informační systémy přinášejí. Na mikropodniky by se neměly vztahovat vůbec.

Není však pochyb o tom, že v případě schválení návrhu směrnice by hospodářské subjekty čelily zvýšení jejich nákladů. V první řadě by musely zajistit, aby technické zabezpečení jejich informačních systémů splňovalo požadavky této směrnice. Další náklady by přineslo vytvoření organizačních opatření k řízení bezpečnostních rizik, tedy vytvoření takových procesů, které by zajistily prevenci proti vzniku bezpečnostních incidentů a minimalizovaly by jejich dopad. Díky vylepšení bezpečnostních kapacit by navíc subjekty zaznamenaly vetší množství bezpečnostních incidentů, na které by musely reagovat, a to by opět znamenalo přírůstek na položce nákladů.[6]

[5] New EU Cyber Security Directive to Impact U.S. Companies. *CIO Journal*. [online]. ©2013. [cit. 2013-03-04]. Dostupné z: http://blogs.wsj.com/cio/2013/02/07/new-eu-cyber-security-directive-to-impact-u-s-companies/.

[6] How will EU cyber security directive affect business? *ComputerWeekly.com*. [online]. ©2013. [cit. 2013-03-04]. Dostupné z: http://www.computerweekly.com/news/2240178256/How-will-EU-cybersecurity-directive.

Neznamená oznamovací povinnost hospodářských subjektů přílišný zásah do jejich práv?

Směrnice stanovuje hospodářským subjektům povinnost podávat odpovědným orgánům zprávy o všech incidentech vážně ohrožujících jejich sítě a informační systémy a majících významný dopad na kontinuitu klíčových služeb a dodávek zboží. Dle Komise jsou informace o incidentech základním předpokladem pro to, aby orgány veřejné správy mohly jednat, přijmout vhodná protiopatření a stanovit odpovídající strategické priority v oblasti bezpečnosti sítí a informací. Důležité je uvést fakt, že to bude Komise, kdo v rámci aktu v přenesené působnosti určí okolnosti, za kterých budou mít hospodářské subjekty oznamovací povinnost.

Směrnice zachází ještě dále, neboť stanovuje, že v případě, že odpovědný orgán rozhodne, že je ve veřejném zájmu, aby byl incident zveřejněn, uvědomí o něm veřejnost. Na toto ustanovení se snesla kritika ze strany mnohých společností, podle nichž by takovéto zveřejnění incidentu mohlo vážně poškodit renomé firmy a způsobit jí tak značné škody. Komise argumentuje tím, že pro plné rozvinutí internetového trhu v Unii je nezbytná důvěra spotřebitelů v online služby. Újma, která může být způsobena dotčené společnosti, je menší než ztráty, které by nastaly v případě nedůvěry zákazníků v celý internetový trh.

Odpovědné orgány by také měly mít k dispozici potřebné prostředky k výkonu svých povinností, včetně pravomoci získat od hospodářských subjektů a orgánů veřejné správy dostatek informací, aby mohly posoudit míru bezpečnosti sítí a informačních systémů, jakož i spolehlivých a úplných dat týkajících se skutečných bezpečnostních incidentů, jež měly dopad na provoz sítí a informačních systémů.

Toto ustanovení je kritizováno z důvodu vágní formulace, neboť nikde není vymezeno či specifikováno, co je „dostatek informací".[7] Navíc, síť pro spolupráci mezi odpovědnými orgány, Komisí a agenturou ENISA by musela absorbovat obrovské množství informací prakticky od všech významných subjektů na internetu.[8]

Je správné vložit veškeré pravomoci do jednoho národního odpovědného orgánu?

Odpovědné orgány by na základě této směrnice disponovaly nemalými pravomocemi. Hospodářské subjekty a orgány veřejné správy by měly povinnost oznamovat odpovědnému orgánu incidenty, jež mají významný dopad na jimi poskytované služby. Členské státy by dále musely zajistit, aby odpovědné orgány měly veškeré nezbytné pravomoci k vyšetřování porušení těchto povinností. Ty budou navíc oprávněny požadovat od těchto subjektů informace, jež jsou nezbytné k posouzení bezpečnosti jejich informačních systémů.

Kritici tohoto návrhu tvrdí, že směrnice odvádí finanční zdroje od policie, které je zodpovědná za řešení kyberkriminality, a dává je zpravodajským agenturám. Namísto toho,

[7] Infosec pros give verdict on EU's new cybersecurity strategy: "Nice try". *Naked security.* [online]. ©2013. [cit. 2013-03-04]. Dostupné z: http://nakedsecurity.sophos.com/2013/02/08/eu-cybersecurity-strategy/?utm_source=dlvr.it&utm_medium=twitter&utm_content=rss2&utm_campaign=Feed.

[8] Comments on the EU Commission's Flawed Cybersecurity Strategy. *We The Net*. [online]. ©2013. [cit. 2013-03-04]. Dostupné z: http://www.wethenet.eu/2013/02/comments-on-the-eu-commissions-flawed-cybersecurity-strategy/.

aby došlo k účinné spolupráci policejních sil, skupin CERT a hospodářských subjektů, vytváří se zde síť vojenských a zpravodajských agentur, která podle mnohých názorů způsobí militarizaci kyberprostoru.[9]

Jaké jsou na návrh směrnice ohlasy ze světa byznysu?

Prakticky všichni aktéři ze světa byznysu se shodnou na tom, že zabezpečení informačních sítí je důležité a nezbytné plnohodnotný rozvoj podnikání. Nad konkrétními ustanoveními této směrnice však již taková shoda nepanuje. Podle některých totiž institut oznamovací povinnosti, podle které by firmy musely odpovědnému orgánu hlásit bezpečnostní incidenty, dostatečně nebere v potaz reputaci společnosti, která je v sázce. Je důležité vytvářet důvěryhodné prostředí v oblasti kybernetického prostoru, avšak tohoto cíle by mělo být dosáhnuto pomocí dobrovolného sdílení informací.

Ovšem ne všechny společnosti se k návrhu staví rozpačitě. Najdou se dokonce i takové, dle jejichž názoru by měla Komise v úpravě této problematiky jít ještě dále. Podle nich je transparentnost a spolupráce klíčová pro plné využití internetového trhu.[10]

Zdroje

Business split over cyber security reporting proposal. iWR. [online]. ©2013. [cit. 2013-03-04]. Dostupné z: http://www.iwr.co.uk/information-management-and-technology/3011481/Business-split-over-cyber-security-reporting-proposal.

Comments on the EU Commission's Flawed Cybersecurity Strategy. We The Net. [online]. ©2013. [cit. 2013-03-04]. Dostupné z: http://www.wethenet.eu/2013/02/comments-on-the-eu-commissions-flawed-cybersecurity-strategy/.

ENDitorial: Questions on the draft Directive on Cybersecurity Strategy. EDRI. [online]. ©2013. [cit. 2013-03-04]. Dostupné z: http://www.edri.org/edrigram/number11.1/cybersecurity-draft-directive-eu.

How will EU cyber security directive affect business? ComputerWeekly.com. [online]. ©2013. [cit. 2013-03-04]. Dostupné z: http://www.computerweekly.com/news/2240178256/How-will-EU-cybersecurity-directive-affect-business.

Infosec pros give verdict on EU's new cybersecurity strategy: "Nice try". Naked security. [online]. ©2013. [cit. 2013-03-04]. Dostupné z: http://nakedsecurity.sophos.com/2013/02/08/eu-cybersecurity-strategy/?utm_source=dlvr.it&utm_medium=twitter&utm_content=rss2&utm_campaign=Feed.

[9] ENDitorial: Questions on the draft Directive on Cybersecurity Strategy. *EDRI*. [online]. ©2013. [cit. 2013-03-04]. Dostupné z: http://www.edri.org/edrigram/number11.1/cybersecurity-draft-directive-eu.

[10] Business split over cyber security reporting proposal. *iWR*. [online]. ©2013. [cit. 2013-03-04]. Dostupné z: http://www.iwr.co.uk/information-management-and-technology/3011481/Business-split-over-cyber-security-reporting-proposal.

New EU Cyber Security Directive to Impact U.S. Companies. CIO Journal. [online]. ©2013. [cit. 2013-03-04]. Dostupné z: http://blogs.wsj.com/cio/2013/02/07/new-eu-cyber-security-directive-to-impact-u-s-companies/.

Plán počítačové bezpečnosti v EU má chránit otevřený internet a svobodu a příležitosti v on-line prostředí. Evropská komise. [online]. ©2013. [cit. 2013-03-04]. Dostupné z: http://ec.europa.eu/ceskarepublika/press/press_releases/13_94_cs.htm.

Special Eurobarometer 390. European commission. [online]. ©2012. [cit. 2013-03-04]. Dostupné z: http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf.

Strategie kybernetické bezpečnosti EU: Otevřený, bezpečný a chráněný kyberprostor. Evropská komise. [online]. ©2013. Dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=JOIN:2013:0001:FIN:CS:PDF.

Autor: Jiří Brada
Imprimatur: Petra Pejchová, Zuzana Netolická
Jazyková úprava: Petra Pejchová
Grafická úprava: Jan Hlaváček
Vydala Asociace pro mezinárodní otázky pro potřeby XVIII. ročníku Pražského studentského summitu.

Model EU

Asociace pro mezinárodní otázky,
Žitná 27, 110 00 Praha 1
Tel./fax: +420 224 813 460,
e-mail: summit@amo.cz,
IČ: 65 99 95 33

»www.amo.cz«
»www.studentsummit.cz«

Top partneři

Generální partner Modelu OSN

The Kellner Family Foundation

Hlavní partner Modelu OSN

G2 OD KOMERČNÍ BANKY

Hlavní partner Modelu NATO

Ministerstvo zahraničních věcí České republiky

Model NATO is co-sponsored by the North Atlantic Treaty Organization

NATO OTAN

Hlavní partner Modelu EU

Evropská komise

Partner konference

Microsoft

Univerzitní partner

Vysoká škola ekonomická v Praze VŠE

Partner zahájení

interhotel AMBASSADOR ZLATÁ HUSA

Partner jednání

KONGRESOVÉ CENTRUM PRAHA

Partneři Modelů

čeps, a.s.

Embassy of Canada
Ambassade du Canada

US embassy

SKUPINA ČEZ

Botschaft der Bundesrepublik Deutschland Prag

Mediální partneři

Hlavní mediální partner

lidovky.cz

RESPEKT

Hlavní mediální partner

LIDOVÉ NOVINY

ISIC INTERNATIONAL STUDENT IDENTITY CARD

Partner Chronicle

METROPOLITNÍ UNIVERZITA PRAHA

ČESKÝ ROZHLAS

Za podpory

Česká televize

Asociace pro mezinárodní otázky
Association for International Affairs

Pražský studentský summit
projekt Asociace pro mezinárodní otázky