IKSP
Institut pro kriminologii
a sociální prevenci

Škody působené kybernetickou kriminalitou

Zpráva shrnující hlavní poznatky Pracovní skupiny k nákladům kyberkriminality

Praha 2019

Ediční řada Prameny

Institut pro kriminologii a sociální prevenci Praha 2019

Škody působené kybernetickou kriminalitou

Zpráva shrnující hlavní poznatky Pracovní skupiny k nákladům kyberkriminality

Přeloženo z anglického originálu „*Understanding the costs of cyber crime. A report of key findings from the Costs of Cyber Crime Working Group: Research Report 96*“, vydaného Home Office Science Advisory Council v lednu 2018. Přeloženo se svolením Úřadu policie Jejího veličenstva (Her Majesty's Stationery Office), který nenese odpovědnost za přesnost tohoto překladu.

Vydal Home Office Londýn
Výzkumná zpráva 96
ISBN 978-1-78655-392-8
ISSN 1756-3666

Překlad:
RNDr. Čeněk Novotný, Mgr. Jiří Vlach, Mgr. Kateřina Kudrlová

Předmluva:
Mgr. Jiří Vlach

Technická redakce:
Lucie Černá

ISBN 978-80-7338-175-2

www.kriminologie.cz

Obsah

Předmluva vydavatele

Spolu se stále širším využívání moderních technologií ve všech oblastech lidské činnosti, můžeme v posledních letech zaznamenat také výrazný nárůst kybernetické kriminality. Vzhledem k tomuto trendu lze předpokládat také značný nárůst nákladů spojených s kybernetickou kriminalitou. Nejedná se však jen o škody způsobené přímým dopadem kybernetických útoků, ale též o náklady na anticipaci a prevenci, jakož i náklady vynaložené v reakci na takové útoky.

Institut pro kriminologii a sociální prevenci v ediční řadě „Prameny" tradičně přináší odborné i laické veřejnosti překlady zahraničních materiálů z oblasti kriminologie. S přihlédnutím k aktuálnosti dané problematiky jsme se rozhodli publikovat překlad zprávy Pracovní skupiny k nákladům kybernetické kriminality (Costs of Cyber Crime Working Group) vydané v edici britského Home Office. Pracovní skupina se pokusila vytvořit rámec umožňující co možná nejpřesnější odhad výše nákladů spojených s kybernetickou kriminalitou. Dosavadní pokusy o takové odhady se potýkaly s mnoha metodologickými problémy a jejich výsledky vykazovaly značnou míru nekonzistentnosti.

Při překladu této zprávy jsme se potýkali s jistými obtížemi pramenícími z multidisciplinární povahy textu. V některých pasážích byli překladatelé nuceni ve snaze o významově co možná nejpřesnější překlad volit poněkud kostrbaté formulace, které však neovlivňují negativně srozumitelnost textu. Věříme, že český překlad této publikace přispěje k hlubšímu poznání problematiky odhadu nákladů kybernetické kriminality a bude inspirací pro další zkoumání zmíněné materie.

Mgr. Jiří Vlach, IKSP

Poděkování

Home Office Analysis and Insight podpořila Home Office Science Advisory Council (HOSAC) tím, že zřídila a zajistila činnost Pracovní skupiny k nákladům kyberkriminality (Costs of Cyber Crime Working Group) v období od podzimu 2014 do jara 2016. Tato zpráva byla sepsána Anthony Cooperem a Samanthou Dowlingovou působícími v HOSAC. Koordinace pracovní skupiny byla prováděna Samanthou Dowlingovou s podporou Toma Buckeho, Sama Branda, Roba Streeta, Sophie Hinde, Seana Millse a Angie Scholes.

Autoři děkují externím členům Pracovní skupiny k nákladům kyberkriminality (Costs of Cyber Crime Working Group): prof. Davovi Delpymu, prof. Davidu Wallovi, prof. Stevovi Furnellovi, prof. Davidu Pymovi, Ruth Daviesové, Ali Imanatovi, Dr. Tomu Holtovi, Dr. Alici Hutchingsové, Emmě Dickensové, Johnu Flatleyovi, Patricku Andersonovi, Garethu Reesovi, Davidu Fysonovi, Tomu Ryderovi, Henry Bryersovi a Dr. Chrisu Feltonovi za jejich příspěvky pro Pracovní skupinu k nákladům kyberkriminality. Poděkování se týká rovněž dalších výzkumných pracovníků, kteří prováděli původní výzkum s cílem odstranit existující mezery ve znalostech: Dr. Adamu Bosslerovi, prof. Mattu Williamsovi, Davidu Emmovi, Dr. Marii Papadaki, Dr. Olze Smirnové, Dr. Maxu Kilgerovi, Caitlin Connorsové, Deboře Willisové, Gurprit Dhillonové, Catherine Grantové a Preriit Soudové. Autoři děkují rovněž klegům z HOSAC, kteří podpořili tento pracovní program a bez jejichž pomoci by tato zpráva nemohla vzniknout.

Význam použitých zkratek

ABS	Annual Business Survey – každoroční obchodní průzkum prováděný ONS v UK
AV	antivirus
AVS	Address Verification Services
BIS	Business, Innovation and Skills
BRC	British Retail Consortium
Cebr	Centre for Economics and Business Research
CIFAS	Credit Industry Fraud Avoidance System, služba v UK zaměřená na potírání podvodů
CJ	CJ marketingová síť
CJS	Criminal Justice System, systém trestní justice
CPNI	Centre for the Protection of National Infrastructure
CSC	Card Security Code
CSEW	Crime Survey for England and Wales, Průzkum kriminality v Anglii a Walesu
CVS	Commercial Victimisation Survey, Výzkum viktimizace subjektů byznysu
DCMS	Department for Culture Media and Sport, Ministerstvo kultury, médií a sporu UK
DCPCU	Dedicated Card and Payment Crime Unit
DDoS	distributed denial of service, distribuované odmítnutí služby
DoS	denial of service, odmítnutí služby
DV	duševní vlastnictví
EU	Evropská unie
FFA UK	Financial Fraud Action UK, organizace spadající pod Obchodní asociaci UK zaměřená na finanční podvody
FISS	Fraud Intelligence Sharing System
HDP	hrubý domácí produkt
HOSAC	Home Office Science Advisory Council
ICT	information and communication technologies, informační a komunikační technologie
ISP	internet service provider, poskytovatel internetového připojení
IT	information technologies, informační technologie
LBE	large business entities, velké podniky
NCA	National Crime Agency
NFA	National Fraud Authority
ONS	Office for National Statistics, Národní statistický úřad UK
PR	public relations, vztahy s veřejností
R & D	research and development, výzkum a vývoj
SME	small and medium-sized enterprizes, malé a střední podniky
TNS BMRB	výzkumná agentura Kantar Public
UK	United Kingdom, Spojené království Velké Británie a Severního Irska.

Shrnutí

Předchozí odhady Home Office týkající se škod způsobených kriminalitou v minulosti kybernetickou kriminalitu nezahrnovaly, a to kvůli snaze provést přesný odhad (Home Office, 2000), avšak v současné době se zvyšuje potřeba porozumět i těmto moderním typům trestné činnosti, potažmo nákladům vzniklým jejich škodlivým působením. Z širšího hlediska je třeba porozumět tomu:

- kam spadají různé škody způsobené kybernetickou kriminalitou (např. do prevence kybernetické kriminality nebo jako reakce na kybernetickou kriminalitu);
- jaké podoby tyto škody nabývají; a
- které subjekty jsou nejvíce postiženy (např. jedinci, oblasti byznysu).

Strategie s názvem Serious and Organised Crime Strategy (Strategie proti závažnému a organizovanému zločinu, Home Office, 2013a) proto přijala závazek vytvořit externí Pracovní skupinu k nákladům kyberkriminality (Costs of Cyber Crime Working Group, dále jen "Pracovní skupina"), která by pomohla zlepšit kvalitu dat reflektujících škody působené kybernetickou kriminalitou. Tato zpráva se nepokouší dospět k celkovému odhadu škod působených počítačovou kriminalitou. Spíše monitoruje činnost Pracovní skupiny s cílem zlepšit kvalitu dat pokrývajících tuto oblast tím, že se specificky zaměřuje na vývoj celkového rámce pro odhad způsobených škod. Ve světle tohoto rámce zpráva přináší řadu doporučení, jak by měl vypadat budoucí výzkum kybernetické kriminality a jejích důsledků. Zpráva byla sepsána proto, aby pomohla výzkumným pracovníkům docílit v budoucích studiích lepších odhadů škod působených kybernetickou1 kriminalitou.

Pracovní skupina sestávala z akademických pracovníků, úředníků z mnoha vládních pracovišť a příslušníků policie a bezpečnostních složek a dalších orgánů zodpovědných za pomoc v boji s kybernetickou kriminalitou. Řídil ji HOSAC a v činnosti byla od podzimu 2014 do jara 2016. Náplň práce Pracovní skupiny zahrnovala kriminalitu přímo spojenou s činností počítačů (např. šíření malwaru, hacking a útoky typu DDoS) a kriminalitu, která je nepřímo umožňována činností počítačů (např. podvod a krádež), tak jak jsou definovány ve Strategii proti závažnému a organizovanému zločinu (Home Office 2013a). Věnovala se rovněž jednotlivcům a organizacím/podnikatelským subjektům, kteří se stali obětí tohoto typu kriminality.

Více než 16měsíční činnost Pracovní skupiny umožnila provedení řady výzkumných studií s cílem pomoci zaplnit mezery týkající se specifických důkazů a otázek spojených s provedením odhadů nákladů a škod. Ty zahrnuly analýzu zdrojů dat, která byla v předchozím období málo vytěžena, a umožnily dospět k následujícím klíčovým poznatkům.

- Nový odhad škod způsobených britské vládě a průmyslu v důsledku celkem 1 250 případů defacementu webových stránek,[1] ke kterým došlo v letech 2007 až 2015, a to ve výši 1,6 milionu britských liber, s průměrnou výší škody přibližně 1 200 liber na jeden případ defacementu.[2]

1 Změna či zkreslení obsahu webových stránek.

2 Je důležité zdůraznit, že škoda se může rok od roku lišit, takže nejde o statické číslo. Odhad byl proveden na základě vzorku zpráv z úložiště zkreslení webových stránek, Zone-H.

- Nový odhad škod způsobených společnostem působícím v UK v důsledku celkem 89 případů nakažení malwarem zahrnutým v seznamu Malware Domain List[3] mezi lety 2009 až 2014, a to ve výši 5,1 milionu britských liber s průměrnou škodou na jedno nakažení malwarem přesahující 57 000 liber.[4]
- Nový odhad ve výši mezi 6,1 až 25,2 milionů britských liber, které vydělaly subjekty, jež zakoupily na otevřeném a dark webu údaje vztahující se k platebním kartám, které následně zneužily. Odhady byly odvozeny ze studie sledující použití ukradených dat zakoupených v podobě výpisů paměti 50 sad podrobných údajů týkajících se platebních karet.
- Nové střední odhady zisku subjektů prodávajících kradená finanční data[5], pohybující se mezi 89 000 a 355 000 liber. V rámci sledovaného vzorku v dark webu prodávající vydělali v průměru částku mezi 24 000 a 95 000 liber.
- Soubor nových opatření pro lepší pochopení a vyčíslení ztrát plynoucích z poškození dobré pověsti v rámci obchodu a podnikání v souvislosti s kybernetickou kriminalitou, spolu s praktickým návodem pro subjekty působící v oblasti byznysu, jak identifikovat a zmírnit dopady potenciálního poškození dobré pověsti.
- Zjištění, že obavy z kybernetické trestné činnosti představují pro subjekt měřitelné „měkké" náklady a škody. Analýza zjistila, že v rámci EU je Velká Británie klasifikována jako šestý stát nejvíce se obávající ekonomické kybernetické kriminality a čtvrtý stát z hlediska obav z kybernetické kriminality související s obsahem. Větší obava panuje z ekonomické kybernetické kriminality než z kybernetické kriminality související s obsahem. Oběti trestné činnosti, ženy, rodiče a ekonomicky znevýhodnění lidé mají podstatně vyšší obavy z kybernetické trestné činnosti než ostatní.

Je třeba vzít v úvahu, že nová čísla vyplývající ze studií předkládaných v této zprávě jsou založena na výzkumu vycházejícím ze vzorků dostupných dat a představují malý podíl pravděpodobných celkových nákladů.

Rámec dělící náklady na anticipaci a prevenci útoku, náklady samotného dopadu útoku a náklady vynaložené v reakci na trestnou činnost, byl vyvinut, aby napomohl konceptualizovat plný rozsah nákladů spojených s kybernetickou kriminalitou a ukázat, jak by další výzkum mohl přistoupit k odhadům těchto nákladů v budoucnosti. Přehled odhadů provedených předchozími výzkumy kybernetické kriminality ukázal, že řada studií nepřesně identifikovala rozsah různých nákladů spojených s nápravou důsledků kybernetické kriminality. Byly použity nekonzistentní definice jak nákladů, tak vlastní kybernetické kriminality a většina studií jednoduše nezjišťovala stejnou věc, a tudíž je srovnání výsledků různých studií obtížné.

Například:
- některé studie se snažily měřit náklady na jeden incident, zatímco jiné měří náklady za rok nebo počítané na postižený subjekt;

3 Zaměřeno pouze na na nakažení malwarem zjištěné na úrovni serverů v UK.

4 Je důležité upozornit, že typ malwaru ovlivňuje individuální náklady a tyto náklady se rok od roku mění, a tudíž se přesné náklady na jednu infekci se od této průměrné hodnoty mohou lišit.

5 Studie bere v úvahu odcizená data z finanční oblasti, která sestávají z 50 sad údajů o platebních kartách.

- podobně některé studie počítaly velké náklady v souvislosti se zcizením duševního vlastnictví, zatímco jiné se o tuto záležitost vůbec nezajímaly.

Jedním z hlavních cílů projektu byla základní úvaha, co by se vůbec mělo zjišťovat a měřit.

Pochopení škály nebo prevalence kybernetické kriminality je rovněž klíčovým požadavkem pro odhad nákladů. Řada dalších pramenů, které následně zlepšily kvalitu dostupných dat, byla publikována během práce Pracovní skupiny a po jejím dokončení. Tyto prameny zahrnují nová experimentální měření kybernetické kriminalityprovedené ze strany Office for National Statistics (ONS) prostřednictvím Crime Survey for England and Wales (CSEW);[6] a rovněž ze strany Department for Culture, Media and Sport's (DCMS) prostřednictvím Cyber Security Breaches Survey.[7] Zatímco tato nová data nebyla v průběhu činnosti Pracovní skupiny k dispozici, je třeba je zahrnout do budoucího odhadování nákladů spojených s kybernetickou kriminalitou.

Ačkoliv je povzbudivé, že stále pokračuje práce zaměřující se na řadu témat, která jsou předmětem výzkumu v této zprávě, je důležité, aby tato činnost reflektovala i její průběžné výsledky. Proto tato zpráva dává rovněž řadu níže uvedených doporučení.

- Budoucí výzkum zabývající se studiemi nákladů kybernetické kriminality by měl být systematický; identifikovat mezery v celkovém rámci odhadu nákladů kybernetické kriminality; a formulovat otázky tak, aby tyto specifické mezery byly zaplněny.
- Budoucí výzkum by se měl zaměřit na nejzávažnější mezery v celkovém rámci nákladů kybernetické kriminality, např. nákladů na prosazování zákona.
- Budoucí studie by měly dále studovat náklady a zisky delikventů působích v oblasti kybernetické kriminality.
- Budoucí studie by měly usilovat o testování měření uvedených v Příloze 3 této zprávy tím, že budou zjišťovat finanční dopad kybernetických útoků na hodnotu dobré pověsti subjektů působících v oblasti byznysu.
- Měla by být provedena další hloubková analýza a co nejlepší využití dat dostupných díky Action Fraud.[8]
- Budoucí výzkum by měl dále uvážit, jak odhadovat peněžní náklady spojené s obavami z kybernetické kriminality.
- Budoucí studie by měly při odhadování nákladů kyberkriminality stále více vycházet z narůstajícího množství solidních dat (např. z měření kybernetické kriminality provedené CSEW nebo dat poskytnutých výzkumem DCMS).

6 Průzkum kriminality v Anglii a Walesu provedený Národním statistickým úřadem UK.

7 Průzkum narušení kybernetické bezpečnosti provedený Ministerstvem kultury, médií a sportu UK.

8 Národní oznamovací centrum pro podvodná jednání a kyberkriminalitu UK.

I.

Úvod

Řada studií provedených v posledních letech se pokouší odhadovat náklady spojené s kybernetickou kriminalitou. Tyto studie jsou ve svém přístupu k odhadu nákladů často nekonzistentní, a jako takové často používají velmi odlišné ukazatele, např. roční náklady, náklady na útok, náklady na sektor. I tam, kde studie používají stejný přístup, jsou konečné výsledky často nekonzistentní – např. Ponemon Institute (2015) odhadl, že průměrné roční náklady spojené s kybernetickou kriminalitou vypočítané pro veřejný sektor v UK v roce 2012 představovaly 1,2 milionu liber, zatímco odhad Detica (2011) pro škody způsobené britské vládě činil 3 miliardy liber za rok. Často citovaný výzkum provedený ze strany Detica/Cabinet Office, který tyto náklady pro UK odhadl na 27 miliard liber, byl široce kritizován (např. Anderson a kol. 2012; Home Affairs Select Committee 2013), což zpochybnilo spolehlivost a přesnost tohoto typu odhadů. Studie od Home Affairs Select Committee (2013) vyjádřila konkrétní obavy z nedostatku přesných a aktuálních údajů, které ukazují rozsah a náklady spojené s působením kybernetické kriminality.

V odpovědi na různé, vzájemně si odporující odhady nákladů spojených s kybernetickou kriminalitou prezentované v literatuře, v publikacích jako *Serious and Organised Crime Strategy* (Home Office, 2013a), přijala vláda stanovisko, že „*přesný odhad rozsahu a nákladů spojených s kybernetickou kriminalitou pravděpodobně nikdy nebude stanoven.*" V rámci téže strategie přijala vláda závazek vytvořit novou externí Pracovní skupinu, která by pomohla zlepšit kvalitu dat týkajících se nákladů spojených s kybernetickou kriminalitou. Tato zpráva se nepokouší dosáhnout celkového odhadu těchto nákladů, spíše se zaměřuje na snahu Pracovní skupiny[9] zlepšit kvalitu dat, se specifickým cílem vytvoření rámce konceptualizace pro co nejlepší vyčíslení uvedených nákladů pro další výzkum. Zpráva zahrnuje činnost prováděnou v období od podzimu 2014 do jara 2016, a proto se nevztahuje na následný výzkum prováděný na toto téma.

Ačkoliv odhadování nákladů spojených s kybernetickou kriminalitou představuje velkou výzvu, Pracovní skupina identifikovala řadu důležitých důvodů pro zlepšení kvality dat v této oblasti. Lepší pochopení škály i nákladů kybernetické kriminality má základní význam pro:

- porozumění povaze hrozby, kterou představuje kybernetická kriminalita, a jak se tato hrozba proměňuje v čase;
- zvýšení povědomí o kybernetické kriminalitě a jejích dopadech na prosazování zákona, a to za účelem pomoci činit informovaná rozhodnutí o prioritách; a
- nasměrování zvýšení tohoto povědomí a preventivního úsilí na ty nejzranitelnější obchodní společnosti a jednotlivce.

V širší souvislosti je důležité pochopit, kam různé náklady spadají (např. do prevence kybernetické kriminality nebo jako reakce na kybernetickou kriminalitu), jakou podobu tyto náklady na sebe berou a koho nejvíce postihují (např. kteří jedinci, které obchodní společnosti).

Předchozí výzkumná zpráva Home Office (2013c) zmiňuje, že zlepšování v odhadech a zaznamenávání kybernetické kriminality je „*kritické pro pochopení, zda rozsah kyber-*

9 Costs of Cyber Crime Working Group (Pracovní skupina k nákladům kyberkriminality, dále jen „Pracovní skupina") působí pod dohledem Home Office Science Advisory Council (HOSAC).

netické kriminality vzrůstá nebo klesá a jak se povaha tohoto problému proměňuje v čase", (str. 14). Government Statistical Service (2011)[10] vyjádřila ve své publikaci *Review of Crime Statistics* obavu, že existující statistiky nezachycují kybernetickou kriminalitu adekvátně. V důsledku toho byl pracovní program týkající se nákladů spojených s kybernetickou kriminalitou realizován v době, kdy řada probíhajících širších změn umožnila lepší přístupnost dat týkajících se kybernetické kriminality z hlediska jejich získávání a vyhodnocování. Office for National Statistics (ONS, 2015) publikoval zprávu o terénním testování nových měření navržených k začlenění do CSEW, a to s cílem zlepšit pochopení škály a rozsahu podvodných jednání a kybernetické kriminality. Bez tohoto pochopení je obtížné činit věrohodné odhady celkových nákladů spojených s kybernetickou kriminalitou.

Pracovní skupina vzala nová fakta v úvahu a snažila se vyhnout duplikacím. Počínaje říjnem 2015 byly nové otázky týkající se kybernetické kriminality zahrnuty do CSEW a poprvé v lednu 2017 byla tato data zahrnuta do celkového šetření CSEW (ONS, 2017), což vedlo k odhadu celkového počtu 2,0 milionu kybernetických trestných činů spáchaných v Anglii a Walesu v kalendářním roce končícím zářím 2016. Toto zjištění výrazně zlepšuje pochopení rozsahu kyberkriminality, ale data bohužel nebyla dostupná během výzkumu prováděného Pracovní skupinou. Podobně revidovalo svůj výzkum pro podnikatelskou sféru nazvaný Cyber Security Breaches Survey i DCMS tím, že zlepšilo použitou metodiku, a tudíž i spolehlivost a přesnost výsledných odhadů, a výsledky nového výzkumu publikovalo poprvé v květnu 2016. Spolu s dalším budoucím vývojem povedou zřejmě tato zlepšení obsáhlých souborů dat vztahujících se i ke kybernetické kriminalitě pravděpodobně ke zlepšení kvality odhadování jejích nákladů, v době činnosti Pracovní skupiny však bohužel zatím nebyla k dispozici.

Pracovní skupina k nákladům kyberkriminality

Pracovní skupina byla zřízena v říjnu 2016 a sestávala z akademických pracovníků, pracovníků mnoha vládních útvarů zabývajících se kybernetickou kriminalitou, příslušníků policie a bezpečnostních složek a pracovníků jiných orgánů odpovědných za úsilí bránit kybernetické kriminalitě. Řídil ji HOSAC a v jejím čele až do konečného zasedání v březnu 2016 stál jeho člen.

Úkolem Pracovní skupiny bylo uspořádat agendu a zaměřit svou činnost na zlepšení kvality získávaných dat a odhadů sociálních a ekonomických nákladů kybernetické kriminality. To zahrnuje lepší pochopení a měření:

- prevalence a/nebo incidence kybernetické kriminality, jejichž znalost je nezbytná pro zlepšení odhadování nákladů; a
- širších újem a dopadů kybernetické kriminality než jen finančních škod.

Působnost skupiny pokrývala trestnou činnost závislou na prostředí ICT i trestnou činnost jím usnadněnou, tak jak je definováno ve strategii Serious and Organised Crime Strategy (Home Office 2013a) a v Kapitole 2.a.[11] Působnost zahrnula jednotlivce i právní subjekty a organizace.

10 Statistická služba vlády UK.

11 Cyber-dependent crime a cyber-enabled crime.

Během šestnáctiměsíčního působení Pracovní skupiny byla uskutečněna řada výzkumných studií:

- literární rešerše k nákladům spojeným s kybernetickou kriminalitou;
- vytvoření rámce pro odhadování nákladů spojených s kybernetickou kriminalitou;
- odhad prevalence a finančních dopadů defacementu webových stránek v UK;
- odhad rozsahu a nákladů způsobených nakažením malwarem v UK;
- odhad zisků a ztrát v souvislosti s nelegálními trhy;
- výzkum rozsahu poškození dobré pověsti subjektů působících v oblasti byznysu v důsledku kybernetické kriminality;
- porozumění rozsahu, trendům a měření kybernetické kriminality; a
- výzkum důsledků obav z kybernetické trestné činnosti.

Souhrny zjištění plynoucích z uvedených studií jsou zde prezentovány, spolu s informací, kde je možné nalézt podrobnější zprávy publikované samotnými výzkumníky.

Tato zpráva je uzavřena diskusí založenou na základě vytvořeného rámce výzkumu nákladů kybernetické kriminality, s využitím různých poučení plynoucích z úkolu navrhnout takový rámec s cílem udat směr budoucího výzkumu v této oblasti.

II.

Souhrn existující literatury

1. Definice

V publikaci *Serious and Organised Crime Strategy* (Home Office, 2013a) vláda UK poukázala na některá témata, která se objevila v souvislosti s kybernetickou kriminalitou, a která umožňují definovat v této souvislosti dva typy trestné činnosti.

„Trestná činnost závislá na využití ICT, tedy počítačová trestná činnost v užším smyslu (cyber-dependent crime): činnost, která může být prováděna pouze s použitím počítačů, počítačových sítí nebo jiných forem informačních a komunikačních technologií. Tato činnost zahrnuje vytváření a rozšiřování malwaru s cílem obohatit se, hacking s cílem zcizit důležitá osobní či průmyslová data a DoS útoky s cílem poškození dobré pověsti subjektu", (str. 22).

„Trestná činnost usnadněná využitím ICT (cyber-enabled crime): činnost, která je prováděna online nebo offline, a je-li prováděna online, může být uskutečňována v mimořádném měřítku a rychlosti", (str. 22).

Příklady trestné činnosti usnadněné využitím počítačů zahrnují podvody včetně hromadných podvodných e-mailů, phishingu a jiných podvodů souvisejících s elektronickým bankovnictvím a obchodováním, a krádeže (včetně krádeží osobních údajů a identifikačních dat).

Existují i jiné klasifikace a definice kybernetické kriminality, např.:

- Anderson a kol. (2012) použil definici, která zahrnuje tradiční formy trestné činnosti, zveřejňování nezákonného obsahu a trestnou činnost spojenou výlučně s elektronickými sítěmi; nebo
- Wall (2007)[12], který definoval kybernetickou trestnou činnost jako trestnou činnost proti stroji / zařízení, trestnou činnost využívající stroje / zařízení a trestnou činnost v rámci stroje / zařízení.

V zájmu konzistence s předchozím výzkumem prováděným ze strany Home Office se bude tato zpráva držet klasifikace na trestnou činnost závislou na využití ICT a trestnou činnost usnadněnou využitím ICT.

Výzkum zde prezentovaný se nezabývá náklady spojenými s kyberterorismem, online trestnými činy z nenávisti, kyberšikanou, porušováním práv duševního vlastnictví nebo online sexuálními trestnými činy. Pracovní skupina se usnesla, že tyto ostatní typy nákladů by měly zůstat mimo její působnost, aby rozsah její práce byl zvládnutelný a přesně zaměřený a aby se zamezilo duplikaci jiných činností probíhajících v této oblasti.

12 Revidováno v květnu 2010 a únoru 2011.

2. Náklady spojené s kybernetickou kriminalitou

V zájmu pochopení široké palety odhadů nákladů zveřejněných v předchozích výzkumech, byla provedena literární rešerše (Dr. Adamem Bosslerem ve spolupráci s Home Office Analysis and Insight) s použitím online vyhledávání odhadů nákladů spojených s kybernetickou kriminalitou v UK, které byly publikovány od zprávy Detica (2011) do 1. ledna 2016.

Celkově přezkoumání ukázalo, že rozsah a povaha odhadovaných nákladů se velmi různí:

- nejvyšší odhad ekonomických nákladů v UK činil 27 miliard liber (Detica, 2011);
- nejnižší odhad nákladů pro subjekty působící v byznysu například 4,1 milionu liber za rok pro 39 subjektů (Ponemon Institute, 2015); a
- velmi specifickou složkou nákladů byly například náklady na clean-up ve výši 0,8 milionu liber (Oxford Economics, 2014).

Studie rovněž používaly různé metody, například:

- škálování zaokrouhlované po 5 % HDP (např. Anderson a kol., 2012);
- odvozování odhadů na základě průzkumu (např. Oxford Economics, 2014);
- odvozování odhadů na základě informací poskytovaných přímo bankami podle schválených definic a kategorií používaných v průmyslu (např. Financial Fraud Action UK, 2015).

Studie používaly různé jednotky měření a typy nákladů, například:

- ekonomické náklady (např. Detica, 2011);
- průměrné roční náklady (např. Ponemon Institute, 2015);
- mediány (např. City of London Police, 2015);
- náklady pro UK (např. National Fraud Authority, 2013); a
- náklady pro podnikatelské subjekty (např. Detica, 2011).

Literární rešerše poukázala na množství obtíží spojených s odhadováním nákladů prezentovaným v existujících výzkumných zdrojích. Mnoho článků používalo odlišné definice nákladů kybernetické kriminality - což často znamenalo, že se studie pokoušely měřit v zásadě odlišné věci. Tato skutečnost nejenže ovlivnila výslednou výši nákladů spojených s kybernetickou kriminalitou, ale rovněž značně ztížila komparaci různých odhadů nákladů spojených s kybernetickou kriminalitou. Kromě těchto rozdílů v definicích se různé studie v literatuře pokoušely měřit velmi odlišné typy nákladů, stejně jako odlišné typy kybernetické kriminality. V některých případech to znamenalo, že určité aspekty kybernetické kriminality vůbec nebyly měřeny – viz například zpráva společnosti Detica (2011), která je zaměřena na velmi úzkou skupinu trestné činnosti.

Byla použita celá řada metod. Některé studie rozlišovaly náklady anticipace, náklady reakce na útok a náklady jeho dopadu (např. Anderson a kol., 2012). Jiné studie používaly širokou škálu metod, které však neumožňovaly srovnání.

Ačkoliv některé studie používaly k získání dat průzkumy formou dotazníků, řada jich vykazovala metodologické slabiny. Například studie provedená Oxford Economics (2014)

nepoužívala náhodný výběr vzorku. Takový metodologický přístup s sebou přináší řadu důsledků, přinejmenším je pro výzkumníky obtížné extrapolovat zjištění na širší populaci. Avšak i tam, kde byl náhodný výběr vzorku proveden, je obtížné odhadovat ztráty, protože mnoho takových odhadů ztrát založených na dotaznících:

- pravděpodobně představuje pouze část zkoumaných jednotlivců/organizací;
- je založeno na neověřených tvrzeních o sobě samém; a
- může být nadhodnoceno vysokými ztrátami, které uvádí pouze malý počet respondentů (Home Office, 2013c).

Velká část odhadu může pocházet pouze od hrstky respondentů, protože rozložení ztrát v rámci populace pravděpodobně není rovnoměrné (Florencio a Herley, 2011). Ve výzkumech, které umožňují dosažení negativních hodnot (např. předvolební výzkumy), se tato chyba působená nerovnoměrnou distribucí měřeného jevu může sama vyrušit. Avšak ve výzkumech, které dosahují pouze pozitivních hodnot (např. výzkumy měřící náklady), tomu tak není, což znamená, že jestliže je stanovena dolní mez, neexistuje žádná horní mez, takže „*odchylka směřuje vždy nahoru*", (str. 2 tamtéž). Navíc vyskytuje-li se sledovaný jev jen vzácně, chyba výpadku návratnosti může být značná, takže lze těžko posoudit rozsah nepřesných dat (např. díky lhaní, přehánění či zkreslení) (str. 2 tamtéž).

Řada studií hodnocených v literární rešerši byly případové studie. Ačkoli poskytují pracovníkům ve výzkumu i v praxi užitečnou informaci o kontextu při odhadech nákladů kybernetické kriminality, nedovolují extrapolaci a nutně nemusí být reprezentativní z hlediska širšího prostředí, v němž se kybernetická kriminalita vyskytuje. I při použití náhodného výběru vede vysoce koncentrovaná povaha ztrát působených kybernetickou kriminalitou k tomu, že „*náhodný výběr populace ještě neznamená náhodný výběr ztrát*" (str. 1 tamtéž).

V některých méně kvalitních studiích jsou dané odhady nákladů založeny na řadě domněnek. Avšak teorie zakládající tyto domněnky a v některých příkladech i domněnky samotné nebyly vždy jasně zdokumentovány. To komplikuje badatelům možnost tyto studie opakovat a znamená to zároveň, že provedené odhady nemohou být spolehlivě verifikovány.

Podobně rešerše zjistila, že použité metodologické přístupy a domněnky někdy neumožňovaly určit přesnost výsledných odhadů nákladů. Příkladem může být přístup použitý ve studii provedené Andersonem a kol. (2012), který odstupňoval odhady na základě britského podílu na světovém HDP. Použití takto povšechného přístupu může mít za následek menší výstižnost některých odhadů oproti těm odvozeným z konkrétního měření aktivity UK.

Rešerší literatury bylo dále zjištěno, že řadě studií chybí dostatečná transparentnost, aby bylo možno důkladně kriticky zhodnotit použité metody a přístupy a případně tyto studie zopakovat. V těchto případech je obtížné přesně odhadnout přesnost a spolehlivost jakýchkoli výsledných měření.

Ačkoli v literatuře nebyl nalezen žádný celkový odhad nákladů spojených s kybernetickou kriminalitou, který by mohl být interpretován s vysokou mírou spolehlivosti, z rešerše dostupné literatury jasně vyplynulo, že některá data byla na rozdíl od jiných relativně kvalitní. Například údaje prezentované ze strany FFA (2015) představují pravděpodobně

poměrně spolehlivá data, na jejichž základě je možné si učinit určitou představu o celkové kybernetické kriminalitě v UK. FFA shromáždila informace, které jim poskytly banky a které se týkaly všech aktuálních podvodů a s nimi spojených ztrát. Kvalita těchto dat je umocněna jejich sdílením v souladu s ujednanými definicemi a kategoriemi používanými v průmyslu.

Na základě této rešerše se následující kapitola zaměřuje na rámec vytvořený v rámci tohoto výzkumného programu za účelem zvýšení kvality budoucích studií zkoumajících náklady spojené s kybernetickou kriminalitou.

Tabulka 1 uvádí souhrn některých klíčových studií, které byly součástí rešerše, spolu s přehledem některých odhadů provedených v jejich rámci. Studie jsou v tabulce 1 seřazeny podle roků publikace, počínaje těmi nejnovějšími. Jestliže bylo v jednom roce publikováno více prací, jsou prezentovány v abecedním pořádku. Podrobnější přehled literatury je uveden v Příloze 1.

Tabulka 1 - Souhrn sledovaných klíčových studií (2011 - leden 2016)

British Retail Consortium,[13] 2015
Přehled
„British Retail Consortium (BRC) je vedoucí obchodní asociace reprezentující maloobchodní subjekty, počínaje velkými obchody se smíšeným zbožím a obchodními domy až po nezávislé subjekty prodávající široký sortiment zboží v centru měst i mimo města, včetně virtuálního prodeje", (str. 2). Výzkum BRC Retail Crime Survey[14] se snaží zaplnit existující mezeru týkající se důkazů, která vyplývá z nedostatku podrobných měření trestných činů spáchaných s cílem poškodit britské podnikatelské subjekty. Ve zprávě autoři definují kybernetickou kriminalitu jako *„aktivitu, která používá internet pro útok na data nebo jiný digitální materiál, nebo případy kdy je primárním motivem útoku narušení systému či služeb"*, (str. 25). Autoři poznamenávají, že většina zahrnutých subjektů byznysu sdělila, že kybernetické útoky *„zůstávají kritickou hrozbou pro tyto subjekty"*, (str. 25).
Odhady klíčových nákladů
Výzkum provedený v letech 2013–2014 zaznamenal 698 184 případů porušení zákona (ne nutně spadajících do kybernetické kriminality) vůči podnikatelským subjektům, které měly za následek ztrátu nebo škodu na majetku. Autoři poznamenávají, že extrapolací tohoto počtu dospěli k číslu 3 miliony předpokládaných případů porušení zákona (opět nikoli pouze náležejících do kybernetické kriminality) proti subjektům v oblasti maloobchodu v uvedeném časovém období. BRC (2015) uvedlo, že celkové náklady spojené s trestnou činností v sektoru maloobchodu v UK v období 2013-2014 činily 603 miliony liber, což představovalo nárůst o 18 % oproti předchozímu roku. Ve zprávě se rovněž uvádí, že většina respondentů prohlašovala, že počty případů kybernetické kriminality byly buď stejné, nebo vyšší ve srovnání s předchozím rokem. Ve své kapitole o podvodech a kybernetické kriminalitě autoři poznamenávají, že velký podíl případů byl spáchán online – zejména pokud se týká činů zahrnujících krádež osobních údajů. Zúčastnění maloobchodníci uvedli, že *„velká většina podvodů s kreditními nebo debetními kartami a jedna třetina podvodů týkajících se zneužití kreditního účtu (account credit fraud) byla spáchána online"*, (str. 23).

13 Britské maloobchodní konsorcium.

14 Výzkum kriminality v maloobchodu.

Klíčové otázky

Autoři zprávy BRC neuvádějí podrobnosti o vytvoření sledovaného vzorku, ale uvedli, že *„pokryl 50 % obratu maloobchodního sektoru a týkal se 1,6 milionu zaměstnanců"* (str. 10). Vzhledem k nedostatku dostupných podrobnějších údajů, které by popisovaly použité metody, není zřejmé, jak jsou výsledky výzkumu spolehlivé, jak reprezentativní z hlediska maloobchodního sektoru jako celku a zda jsou učiněné extrapolace platné.

Centre for Economics and Business Research (Cebr),[15] 2015

Přehled

Zpráva Centre for Economics and Business Research za rok 2015 poskytuje informace o tom, jak vnímá kybernetickou bezpečnost a náklady spojené s kybernetickými útoky tzv. C-level (hovorový výraz pro vrcholný management obvykle nazývaný ředitelé).

Odhady klíčových nákladů

Cebr odhadlo, že kybernetické útoky způsobily ztráty příjmů firem v UK ve výši 18 miliard liber. Firmy navíc utratily téměř 16 milionů liber v následných platbách IT sektoru v reakci na narušení kybernetické bezpečnosti.

Klíčové otázky

Poznatky z této studie jsou založeny na online výzkumu pracovníků v C-levelu. Ze studie není jasné, jak byl zkoumaný vzorek vybírán, jak reprezentativní byl z hlediska širší populace nebo kolik oslovených ve výzkumu opravdu odpovědělo. Proto není jasné, do jaké míry lze výsledky studie generalizovat.

Financial Fraud Action UK (FFA UK), 2015

Přehled

FFA UK publikuje pravidelné zprávy týkající se ztrát v důsledku různých forem podvodů v oblasti bankovnictví a platebních karet. Shromažďuje a třídí informace poskytované bankami a zahrnuje podrobnosti o všech aktuálních podvodech a s nimi spojených ztrát, v souladu s ujednanými definicemi a kategoriemi používanými v průmyslu.

Odhady klíčových nákladů

FFA UK oznámila, že ztráty vyplývající z podvodů, jež se týkaly karet vydaných v UK, dosáhly v roce 2014 celkové sumy 479 milionů liber, což představovalo 6 % nárůst proti předchozímu roku. Z toho 217,4 miliony liber představovaly podvody spojené s internetovým obchodem a 60,4 milionů liber podvody v oblasti internetového bankovnictví.

Klíčové otázky

Data publikovaná FFA UK patří v současné době pravděpodobně k těm nejspolehlivějším, která jsou k dispozici a na jejichž základě můžeme začít odhadovat celkové náklady spojené s kybernetickou kriminalitou v UK. Je to umožněno porovnáváním informací přímo poskytovaných bankami, subjekty vydávajícími kreditní karty, debetní karty a tzv. úvěrové karty, a dále těmi, kdo inkasují platby kartami v UK, přičemž se tyto informace týkají všech aktuálních případů podvodů a s nimi spojených ztrát. Data jsou shromažďována v souladu s definicemi a kategoriemi používanými v průmyslu a kromě toho, že FFA UK umožňuje provádět odhady, rovněž přispívá k diskusím o tom, jakým způsobem jsou podvody páchány, a poskytuje informace pro spotřebitele, jak dosahovat vyšší bezpečnosti.

Zpráva FFA UK však neobsahuje podrobnosti o tom, jak byly publikovaná čísla a náklady shromážděny a uspořádány. Dále zpráva uvádí řadu opatření, která subjekty zajišťující platební styk pomocí karet v minulých deseti letech přijaly, a která údajně snížila ztráty působené podvody. Například Dedicated Card and Payment Crime Unit (DCPCU) uvádí, že od svého založení zabránila ztrátám ve výši 470 milionů liber. Už však chybí odhady nákladů této činnosti. Ty by poskytly lepší porozumění nákladům vynaloženým na anticipaci či prevenci různých forem podvodů.

15 Centrum pro ekonomický a obchodní výzkum.

Neustar, 2015

Přehled

Ve své zprávě z roku 2015 Neustar (poskytovatel celosvětových informačních služeb působící v USA) prezentuje zjištění svého výzkumu provedeného IT odborníky, který měl za cíl odhadnout současné hrozby a dopady útoků v oblasti byznysu, jež mají za následek DOS a DDoS.

Odhady klíčových nákladů

Ve svém vzorku 250 odborníků Neustar (2015) zjistil, že 22 % společností ohlásilo ztráty příjmů ve výši mezi 50 000 a 99 999 liber za hodinu v důsledku výpadku provozu ve špičce (šlo o nejčastější odpověď). 16 % společností oznámilo, že jejich ztráty přepočtené na hodinu byly menší než 30 000 liber, 12 % oznámilo ztráty mezi 30 000 a 49 999 librami, 16 % ztráty mezi 100 000 a 299 999 librami, 11 % ztráty mezi 300 000 a 600 000 librami, 12 % ztráty vyšší než 600 000 liber a 11 % nevědělo, kolik je výpadek provozu vlastně stál.

Klíčové otázky

Z informace uvedené ve zprávě nebylo možno odhadnout, jak reprezentativní jsou tato zjištění z hlediska širší odborné veřejnosti.

Ponemon Institute, 2015

Přehled

Studie Ponemon Institute (2015) týkající se nákladů společností v UK spojených s kybernetickou kriminalitou zkoumala celkové náklady, které musely organizace zaplatit v souvislosti s kybernetickými útoky. Náklady zahrnovaly detekci, vyšetřování a vyhrocení útoku, zamezení šíření, obnovu, následnou reakci a snahy snížit vliv útoku z hlediska ztráty informací nebo jejich zcizení, poškození činnosti subjektu, poškození vybavení a ztráty příjmů. Studie je prováděna jednou ročně a zpráva hodnotí změny v čase.

Metodologie použitá Ponemon Institute zahrnula 326 interview se zaměstnanci 39 velkých organizací. Jak autoři ve zprávě konstatují, *„každá roční studie zahrnuje různý vzorek subjektů. Jinými slovy, nesledujeme stejný vzorek subjektů v čase"*, (str. 2). Proto rozdíly mezi odhady z roku na rok mohou reflektovat spíše rozdíly mezi subjekty než skutečné změny nákladů.

Odhady klíčových nákladů

Ponemon Institute v roce 2015 zjistil, že průměrné roční náklady pro 39 korporací činily 4,1 milionu liber za rok (medián 3,4 milionu liber), což reprezentovalo 14 % přírůstek oproti roku 2014, v rozmezí mezi 628 423 a 16 miliony liber.

Klíčové otázky

Je výslovně uvedeno, že cílem výzkumníků není poskytnout odhady, které mohou být generalizovány jako celkové náklady spojené s kybernetickou kriminalitou v rámci ekonomiky UK, ale spíše poskytnout data o *„zkušenostech společností v UK s kybernetickými útoky a o širším prostředí kybernetických útoků"*, (str. 3). Některá z omezení týkající se tohoto výzkumu spočívají v tom, že Ponemon Institute (2015), podobně jako jiné společnosti, používal svou vlastní srovnávací metodu nedovolující vnější přezkoumání. Navíc jeho metodologie zahrnuje:

- vzorek, který nedovoluje činit statistické závěry;
- zkreslení v důsledku non-response;
- způsob výběru vzorku, o němž Ponemon Institute předpokládal, že zahrnuje společnosti s vyspělejšími informačními bezpečnostními programy; a
- spoléhání se na čestnost respondentů.

Verizon, 2015

Přehled

Verizon (technologická společnost s celosvětovou působností sídlící v USA) byla ve své zprávě z roku 2015 schopna poskytnout odhad předpokládaných finančních nákladů na základě zcizených záznamů pro subjekty, u nichž došlo k prolomení ochrany dat. Zpráva se týkala 70 organizací v 61 státech vztahujících v roce 2014. Bylo zaznamenáno 79 790 bezpečnostních incidentů (definovaných jako jakákoli událost, která narušila důvěrnost, integritu nebo dostupnost informační položky) a 2 122 potvrzených případů prolomení ochrany dat (definovaných jako incident, jehož výsledkem bylo potvrzené prozrazení neautorizovanému subjektu, nikoli jenom ohrožení).[16]

Odhady klíčových nákladů

Autoři předpovídají náklady prolomení ochrany dat na základě rozsahu prolomení, měřeno počtem ukradených záznamů (100; 1 000; 10 000; 100 000; 1 000 000; 10 000 000; 100 000 000). Například suma 1 258 670 US dolarů představuje očekávané finanční náklady společnosti v souvislosti s odcizením 1 milionu záznamů (průměr byl mezi 892 400 a 1 775 350 USD a odhad mezi 57 600 a 27 500 090 USD).

Klíčové otázky

Autoři poznamenávají, že ačkoli se domnívají, že mnoho jejich zjištění může být generalizováno, nemohou odhadnout míru výběrového zkreslení.[17] Neuvádějí jasně, jaká část všech případů prolomení ochrany dat je zachycena ve výzkumu, poněvadž neznají jejich celkový počet ve všech organizacích – mnoho takových případů nebylo oznámeno nebo nastaly bez povšimnutí.

McAfee / Intel, 2014

Přehled

Ve zprávě McAfee/Intel (2014) se autoři pokusili odhadnout celosvětové náklady spojené s kybernetickou kriminalitou za použití existujících odhadů z předchozích studií. Autoři poznamenávají, že jejich odhad *„se zaměřuje na přímé i nepřímé náklady a na data, která berou v úvahu ztrátu duševního vlastnictví, odcizení majetku a citlivých obchodních informací, náklady obětované příležitosti, dodatečné náklady na zabezpečení sítě a náklady na odstranění následků kybernetických útoků včetně poškození dobré pověsti subjektu vystaveného hackerskému útoku"*, (str. 4).

Odhady klíčových nákladů

Autoři uvádějí, že celosvětové náklady spojené s kybernetickou kriminalitou mohou být 375 miliard dolarů (konzervativní odhad získaný extrapolací dat z otevřených zdrojů, 445 miliard USD (odhad získaný souhrnem nákladů coby podílů regionálních příjmů) nebo až 575 miliard USD (extrapolace dat ze ztrát zemí s vysokými příjmy.

Zpráva McAfee/Intel neudává odhad nákladů spojených s kybernetickou kriminalitou pro UK. Autoři udávají, že podíl HDP UK, který je ztracen v důsledku kybernetické kriminality, je 0,16 % - tato hodnota má nízký interval spolehlivosti.

Klíčové otázky

Tak jako u všech zpráv publikovaných výrobci/dodavateli softwaru, čtenáři si musí být vědomi toho, že jsou vytvářeny s cílem posílit hodnotu jejich produktů a zvýšit potřebu subjektů mít je k dispozici. Výzkum se zaměřuje zejména na předchozí studie, publikované např. Andersonem a kol. (2012), spíše než na nový primární výzkum.

16 Verizon používá jinou terminologii než zákon o kybernetické bezpečnosti (zákon č. 181/2014 Sb.) – pozn. překl.

17 Zkreslení plynoucí ze špatného výběru vzorku – pozn. překl.

Oxford Economics, 2014

Přehled

Studie provedená ze strany Oxford Economics vytvořila ekonomický rámec k pochopení dopadů státem sponsorovaných kybernetických útoků na firmy v UK. Věnuje se britským firmám s cílem odhadnout náklady spojené s kybernetickými útoky a zahrnuje případovou studii, která zkoumá dopad kybernetických útoků na tržní prostředí. Obsahuje též řadu případových studií dokládajících zkušenosti britských firem s kybernetickými útoky.

Výsledky výzkumu prezentované ve zprávě jsou založeny na online dotazníku distribuovaném e-mailem na adresy uvedené v databázi IT odborníků, IT pracovníků zaměřených na bezpečnost a dalších IT specialistů. Z celkem 9 973 rozeslaných dotazníků jich bylo zodpovězených 427, přičemž návratnost 4,3 % bylo autory hodnoceno jako nadprůměrné pro tento obor. S ohledem na způsob výběru nemohou být výsledky tohoto výzkumu považovány za reprezentativní z hlediska firem v UK jako takových.

Odhady klíčových nákladů

Příklad odhadu nákladů uvedený ve zprávě zahrnuje průměrné adjustované náklady britských firem spojených s kybernetickými útoky za 24 měsíců před provedením výzkumu: 0,8 milionu liber za vyčistění/remediaci, 0,9 milionu liber na ztrátu produktivity, 0,18 milionu liber za přerušené operace, 0,8 milionu liber vynaložených na poškození/krádež IT a 0,9 milionu liber za poškození pověsti a obchodní značky.

Zpráva dále zahrnula medián nákladů spojených s kybernetickými útoky vykázanými firmami v UK za 24 měsíců před zahájením výzkumu: 0.18 milionu liber za vyčistění/remediaci, 0,18 milionu liber na ztrátu produktivity, 0,18 milionu liber za přerušené operace, 0,18 milionu liber za poškození/krádež IT a 0,38 milionů liber za poškození pověsti a obchodní značky.

Klíčové otázky

Autoři uzavírají, že přestože výsledky ve zprávě nelze generalizovat, mohou vést k závěru, že ačkoli pouze menšina subjektů byznysu utrpí takové ztráty, výše těchto ztrát převyšuje ostatní náklady vznikající jako následek kybernetických útoků.

National Fraud Authority, 2013

Přehled

National Fraud Authority (NFA) pracovala se zainteresovanými osobami v různých sektorech a učinila celkové odhady na základě primárních dat získaných výzkumem a sekundárních dat od svých partnerů.

Odhady klíčových nákladů

Zpráva NFA (2013) odhaduje náklady spojené s podvody v rámci ekonomiky UK na 52 miliard liber. Toto číslo, jako mnoho jiných ve zprávě, není rozděleno na podvody prováděné online a offline. Zpráva odhaduje, že škoda způsobená charitativním organizacím byla ve výši 147,3 milionu liber a byla učiněna jak online, tak offline způsobem, včetně podvodů při platbách, podvodů učiněných zaměstnanci a dobrovolníky a kybernetických podvodů. Jiné odhady poskytují lepší vhled do podílu podvodů usnadněných díky ICT. NFA např. odhaduje, že roční ztráty finančního sektoru skrze podvody činily 5,4 miliardy liber, z čehož 40 milionů liber byly podvody spojené s online bankovnictvím a 388 milionů liber podvody spojené s užíváním plastových karet. Ztráty způsobené podvody jednotlivcům činily 9,1 miliardy za rok. NFA rozdělila tento odhad na hromadné marketingové podvody představující sumu 3,5 miliardy liber (velká část z této částky byla pravděpodobně způsobena kybernetickými podvody), podvody spojené s identitou, které představovaly 3,3 miliardy liber (značnou část rovněž tvořily kybernetické podvody), podvody s prodejem lístků na internetu (ve výši 1,5 miliardy liber (vše kybernetické podvody), podvody týkající se nájemného ve výši 755 milionů liber a podvody s předplacenými měřiči elektřiny, jejichž suma činila 2,7 milionu liber.

Klíčové otázky

Zpráva NFA (2013) uvádí, že její odhady nutně nemusí být srovnatelné z roku na rok vzhledem k vylepšování metodologie. Proto by měly být považovány za *„nejlepší odhad možné velikosti problému"*, (str. 4).

Odhady prezentované ve zprávě NFA používají:
- sekundární data, z nichž ne všechna jsou spolehlivá;
- výzkumy využívající nenáhodný výběr vzorku, které proto pravděpodobně nejsou reprezentativní; a
- data uvádějící střední průměrné ztráty, která jsou pravděpodobně zkreslena anomáliemi.

Symantec, 2013

Přehled

Společnost vyrábějící bezpečnostní software Symantec podobně publikovala odhady nákladů spojených s kybernetickou kriminalitou jako část své zprávy Norton Report (2013). Tato zpráva představuje výzkumnou studii zaměřenou na chování spotřebitelů a na náklady spojené s kybernetickou kriminalitou.

Odhady klíčových nákladů

Autoři uvádějí, že celosvětové celkové náklady (zahrnující celkem pouze 24 zemí) spojené s kybernetickou kriminalitou v minulých 12 měsících činily 113 miliard US dolarů, přičemž průměrné přímé náklady vypočítané na subjekt postižený kybernetickou kriminalitou činily 298 USD. Pro UK autoři odhadují, že celkové náklady spojené s kybernetickou kriminalitou za minulých 12 měsíců činily 1 miliardu USD s průměrnými přímými náklady vypočítanými na subjekt postižený kybernetickou kriminalitou ve výši 101 USD. Podle jejich odhadu bylo v UK postiženo 12 milionů osob ve věku 18-64 let za posledních 12 měsíců předcházejících výzkumu.

Klíčové otázky

Výzkum v této zprávě zahrnul malý britský online vzorek – obvyklá omezení týkající se zobecnění výsledků vyplývají z tohoto metodického přístupu. Jak je uvedeno výše, jestliže interpretujeme zprávy publikované producenty/dodavateli softwaru, musí si být čtenář vědom toho, že taková zpráva je sepsána proto, aby podpořila potřebu/hodnotu nabízených produktů.

Anderson, Barton, Bohme, Clayton, van Eeten, Levi, Moore and Savage, 2012

Přehled

Pro analýzu nákladů spojených s kybernetickou kriminalitou autoři odhadli celosvětové částky. Pracovali s předpokladem, že UK reprezentuje přibližně 5 % světového HDP a podle toho nastavili odhady jednotlivých států. Autoři uvádějí, že tam, kde tento přístup nebyl vhodný, je to ve zprávě uvedeno, a *„je na tuto skutečnost brán patřičný ohled"*.

Anderson a kol. (2002) navrhli přístup, kdy oddělili přímé a nepřímé náklady. Studie zahrnula rovněž náklady na zabezpečení, náklady pro společnost a náklady příležitosti snížené důvěryhodnosti online transakcí. Náklady použité v analýze byly získány z různých mezinárodních výzkumů, statistických zdrojů a případových studií. Tam, kde bylo zapotřebí, se autoři dobrali různých odhadů nákladů pro UK pomocí domněnek.

Odhady klíčových nákladů

Anderson a kol. (2012) odhadli celkové náklady na prosazení práva v UK v souvislosti s kybernetickou kriminalitou na 15 milionů USD. Autoři rovněž odhadli, že náklady firem na ochranu před kybernetickou kriminalitou v UK představovaly 500 milionů USD a podobná suma byla uživateli v UK vynaložena na odstranění následků útoků.

Klíčové otázky

Je obtížné odhadnout spolehlivost řady odhadovaných hodnot. Zčásti je to z důvodů závislosti na práci ostatních, kteří zjišťují dílčí hodnoty, na nichž je postavena analýza. Publikace představuje důležitý krok vpřed ve vývoji lepšího metodického přístupu či rámce pro odhad nákladů (Home Office, 2013c). Omezení daná použitým přístupem jsou definována jinde: *„výpočet odhadů pro UK vycházející z podílu na celkových nákladech kriminality ve vztahu k HDP závisí jak na přesnosti použitých celosvětových odhadů, tak na předpokladu, že relativní část trestných útoků v UK vždy odpovídá jejich nákladům v poměru k HDP"*, (Home Office, 2013c).

Měli bychom zmínit, že zpráva Andersona a kol. nezahrnuje čísla pro průmyslovou kybernetickou špionáž a vydírání, poněvadž *„není žádný spolehlivý důkaz o rozsahu nebo nákladech spojených s průmyslovou kybernetickou špionáží a vydíráním"*, (str. 18). Předpokládáme-li však, že tento odhad zahrnuje velkou část (2,2 miliardy liber) celkového odhadu nákladů spojených s kybernetickou kriminalitou uvedeného ve zprávě Detica (2011), pak nezahrnutí kybernetické špionáže a vydírání do odhadů ve zprávě Andersona a kol. částečně vysvětluje značné rozdíly v celkových odhadech.

Detica, 2011

Přehled

Tento výzkum se zaměřuje na:
- podvody spojené s krádeží identity a online podvody;
- krádeže duševního vlastnictví (DV);
- špionáž a vydírání; a
- fiskální podvody proti vládě.

Studie je založena na současném nástinu nákladů od roku 2010 a zahrnuje vývoj kauzálního modelu spojujícího kybernetickou kriminalitu s jejími dopady na ekonomiku UK. Tento model byl následně použit pro mapování typů kybernetické kriminality z hlediska kategorií jejich ekonomického dopadu. Model tak lze použít k výpočtu velikosti nákladů spojených s kybernetickou kriminalitou při použití tříčíselného odhadu: scénáře zohledňující nejhorší případy, nejpravděpodobnější případy a nejlepší případy.

Odhady klíčových nákladů

Zpráva uzavírá, že podle nejpravděpodobnějšího scénáře byly odhadované náklady spojené s kybernetickou kriminalitou v UK 27 miliard liber, přičemž autoři upozorňují, že tento odhad je pravděpodobně příliš nízký.

Klíčové otázky

Existuje řada omezení spojených s odhady Detica. Řada z nich se vztahuje k předpokladům, které autoři zprávy učinili a které hrály důležitou roli v tom, jaké byly odhady publikované ve zprávě. Příklady předpokladů jsou následující:
- pouze 1 z 15 událostí je oznámena občany;
- 25 % podvodů s falešnou identitou, je spácháno online; a
- všechny nelegální útoky zaznamenané v NFA Annual Fraud Indicator[18] byly kybernetické útoky.

Dále byla Deticou provedena řada metodologických rozhodnutí, která mohla ovlivnit spolehlivost výsledků. Například rozhodnutí nevzít v úvahu náklady spojené s tím, že firmy bohaté na duševní vlastnictví navyšovaly svoji kybernetickou ochranu (protože autoři pokládali tyto náklady za související s obvyklým podnikáním), nebo rozhodnutí vyloučit náklady vázané na jednotlivce při předvídání kybernetické kriminality (např. firewall, antivirus). Tyto úvahy posilují obavy ohledně spolehlivosti celkového odhadu nákladů ve výši 27 miliard liber, stejně jako různých nižších odhadů, které přispěly k tomuto celkovému výpočtu.

18 Roční indikátor podvodů.

III.

Mapování nákladů spojených s kybernetickou kriminalitou

1. Náklady spojené s kriminalitou

Odhad nákladů spojených s bojem proti kriminalitě může hrát důležitou roli v pomoci vládě při rozhodování, jak v tomto směru vynaložit peníze co nejúčinněji. Odhady mohou být použity pro posouzení a evaluaci strategií snižování kriminality. Mohou vládě pomoci stanovit priority při směřování omezených finančních prostředků na ty strategie, které mají největší dopad na snížení škod působených trestnou činností a nejen na prosté snížení počtu trestných činů (Home Office, 2000, str. 7). Home Office v předchozím období publikoval výzkum společenských nákladů spojených s tradiční kriminalitou, jako jsou loupeže a násilné trestné činy. Home Office (2013 b) rovněž publikoval zprávu odhadující sociální a ekonomické náklady na potlačování vlivu organizovaného zločinu. Vzhledem k problémům spojeným s možností spolehlivě vypočítat tyto náklady však nebyla kybernetická kriminalita dosud v takovýchto odhadech zahrnuta. Ve světle toho, jak se vynořují nové hrozby trestných činů usnadněných ICT a závislých na ICT, vzniká zde potřeba zmapovat důsledky nových moderních typů kriminality a pokusit se kvantifikovat náklady, které tato situace staví před ekonomiku UK.

Výzkum nákladů spojených s trestnou činností se opakuje a zahrnuje publikaci novými zjištěními spolu s tím, jak se zlepšuje metodika a odhady zpřesňují. To pohání zlepšení budoucího výzkumu a shrnuje nejlepší známé odhady nákladů pro účely výzkumné komunity způsobem, který je snadno přístupný.

Při kalkulaci odhadů se výzkum nákladů spojených s trestnou činností zaměřil na ekonomické náklady způsobené UK v přepočtu na jednu událost a odděleně na odhady prevalenci trestné činnosti, a to za účelem celkového pochopení nákladů spojených s trestnou činností. Náklady zahrnuté v tomto výzkumu byly rozděleny do tří kategorií:

- náklady anticipace;
- náklady dopadu; a
- náklady vynaložené v reakci.

Metodologický přístup, vypracovaný předchozí studií nákladů spojených s trestnou činností, byl základem přístupu použitého ve výzkumu nákladů spojených s kybernetickou kriminalitou, který je prezentován v této zprávě.

2. Ekonomické koncepty

Pracovní skupina na základě poznatků z provedené literární rešerše a ve snaze zajistit konzistentnost budoucího výzkumu pracovala na projektu, ve kterém se pokusila formulovat rámec nákladů spojených s kybernetickou kriminalitou tak, aby shrnula a dospěla k lepšímu pochopení různých odhadů nákladů spojených s kybernetickou kriminalitou. Na tomto projektu se podílel Dr. Adam Bossler, spolu s Home Office Analysis and Insight. Přístup byl založen na postupu použitém v předchozím výzkumu provedeném Home Office, který byl zaměřen na náklady spojené s trestnou činností, a rozčlenil náklady do stejných tří kategorií:

- náklady anticipace;
- náklady dopadu; a
- náklady vynaložené v reakci.

Tato kapitola naznačuje ekonomické koncepty, z nichž vychází celkový rámec a popisuje samotný rámec. Následující kapitoly této zprávy pak diskutují, jak může být navržený rámec využit ve výzkumu k zajištění toho, aby budoucí studie byly svým přístupem komplementární a konzistentní.

Zmíněný projekt používá konceptu ekonomických nákladů k tomu, aby ukázal plný dopad kybernetické kriminality na ekonomiku UK. Ekonomické koncepty byly převzaty z metodického návodu publikovaného v roce 2003 ministerstvem financí UK (tzv. Zelená kniha - *Green Book*). Klíčovým konceptem použitým v celém rámci nákladů spojených s kybernetickou kriminalitou jsou náklady příležitosti. Ty se vztahují k tzv. „*nejhodnotnější alternativě*"[19], která v podstatě znamená hodnotu peněz nebo zdrojů, kdyby byly použity jinde místo toho, aby byly přisouzeny v tomto případě kybernetické kriminalitě. Koncept nákladů příležitosti dovolil položit důraz na zdroje, jako jsou lidé či peníze, které by bylo možno použít jinak, pokud by v UK žádná kybernetická kriminalita neexistovala.

Je třeba též vzít v úvahu transfery prostředků. Transfery v ekonomice zahrnují jiné platby než za zboží a služby. To může zahrnovat takové transakce, jako jsou subvence či hazard. Transfery nejsou zahrnovány do nákladů kriminality, neboť nejsou vnímány jako ztráta pro společnost a berou se prostě jako pohyb peněz skrze ekonomiku UK. Příkladem transferů vztahujících se k nákladům spojeným s kybernetickou kriminalitou jsou pokuty uložené obchodním společnostem za nedostatečné zabezpečení dat před kybernetickými útoky. Tyto pokuty nejsou vnímány jako náklady kyberkriminality, nýbrž pouze jako finanční náklady pro firmy.

Podle metodického návodu Home Office rovněž nejsou do nákladů spojených s kybernetickou kriminalitou započteny pojistné platby obětem kybernetické kriminality. Tento návod nezapočítává pojistné škody, neboť nepovažuje transfery peněz mezi oběťmi a pojišťovnami, jakož i kompenzaci obětem od pojišťoven, jako ztrátu pro společnost. Ačkoliv samotné nároky na pojistné plnění nejsou zahrnuty v nákladech spojených s kybernetickou kriminalitou, náklady na administrativu pojišťoven započteny jsou. Představují náklady na zaměstnance, budovy a zařízení, které pojišťovny platí, a představují tak pro společnost náklady příležitosti, neboť kdyby neexistovala kybernetická kriminalita, byly by tyto zdroje uvolněny a použity jinde.

3. Rámec nákladů spojených s kybernetickou kriminalitou

Jak již bylo uvedeno, jsou náklady rozděleny do tří kategorií tak, aby odlišily jednotlivé fáze, určující, jak oběti této trestné činnosti vnímají náklady kybernetické kriminality:

- náklady anticipace;
- náklady dopadu; a
- náklady vynaložené v reakci.

Náklady anticipace jsou běžná obranná opatření, která přijíjají jednotlivci a obchodními společnostmi s cílem předejít trestné činnosti. Příkladem mohou být náklady na antivirový software.

19 HM Treasury: *Green Book*, Slovník pojmů.

Náklady dopadu zahrnují náklady, které jsou okamžitým výsledkem trestné činnosti a běžně na sebe berou podobu škody na majetku nebo finanční ztráty. Mohou však rovněž zahrnovat emocionální či fyzickou újmu způsobenou trestnou činností. Jde o náklady, které mohou ovlivnit jednotlivci jen málo nebo vůbec.

Náklady vynaložené v reakci zahrnují výsledek rozhodnutí, jak reagovat na specifickou trestnou činnost. Typicky zahrnují činnost policie a systému trestní justice, přičemž je zatěžují a představují ztrátu nákladů příležitosti v důsledku kybernetické kriminality. Jde o náklady, které lze lépe řídit s ohledem na potřebnou činnost.

Rámec nákladů spojených s kybernetickou kriminalitou je pokusem udělat přehled všeho, co je o těchto nákladech známo, což by umožnilo lépe pochopit rozdíly ve výsledcích současných výzkumů (míněno v roce 2016) a podpořilo budoucí výzkum. Záměrem bylo umožnit badatelům identifikovat různé složky nákladů spojených s kybernetickou kriminalitou a jak je zkombinovat tak, aby zahrnuly náklady celkově – tento zdroj informací dosud v literatuře neexistoval. Tím bychom měli pomoci badatelům v budoucnu identifikovat slabá místa výzkumu a usnadnit formulaci konzistentního výzkumu, který by mohl být použit pro lepší porozumění celkových nákladů spojených s kybernetickou kriminalitou vůbec. Rámec shrnující rozsah složek těchto nákladů je nastíněn v Tabulce 2. Typy nákladů zahrnutých v tomto rámci vzešly jak z konzultací s analytiky Home Office a Pracovní skupiny, tak také z poznatků získaných literární rešerší.

Tabulka 2 - Rámec nákladů spojených s kybernetickou kriminalitou – souhrn typů nákladů

Náklady anticipace
Technologické náklady
• Software/produkty zajišťující bezpečný provoz počítače (např. antivirus, záplatování) • Zavedení/přidání technologií
Školení
• Školení/vzdělávání v oblasti kybernetické bezpečnosti • Výcvik policejních vyšetřovatelů a důstojníků • Školení soudního a právního personálu
Bezpečnostní praktiky / chování
• Implementace zásad kybernetické bezpečnosti • Vliv zvýšených bezpečnostních opatření na uživatele a obvyklé používání • Výměna poskytovatelů internetových služeb (ISP), poskytovatelů bezpečnostních opatření nebo produktů za účelem zvýšení bezpečnosti • Bezpečnostní prověření zaměstnanců a dodavatelů • Sledování zabezpečení třetích stran • Prověřování úvěrových záznamů/výsledků • Vyhýbání se používání internetu a/nebo jiných technologií (mezi neuživateli[20])
Vládní aktivity
• Návrh a tvorba nové legislativy • Snaha vzdělávat veřejnost v nové legislativě • Realizace národních kampaní na zvyšování povědomí/ochrany
Jiné
• Správa pojištění kybernetických rizik • Služby zajišťující ochranu spotřebitele a identity (např. organizace CIFAS chránící před podvody) • Obavy/strach z kybernetické kriminality • Shromažďování statistických údajů o kybernetické kriminalitě
Náklady dopadu
Náklady na řešení útoku
• Poškození zařízení/infrastruktury • Výdaje na clean-up • Korigování úvěrových záznamů/výsledků
Finanční ztráty
• Narušení obchodní činnosti, včetně ztráty produkce • Online krádež/podvod týkající se finančních zdrojů • Ztracená hodnota duševního vlastnictví/obchodně citlivých informací • Poškození dobré pověsti nebo hodnoty obchodní značky • Sporné transakce

20 Osoby, jež nikdy internet nepoužívaly.

Jiné
• Emoční/fyzické újmy • Služby na podporu obětí
Náklady vynaložené v reakci
Reakce systému trestní justice
Prosazení práva
• Vyšetřování a vymáhání práva
Soudy
• Soudní stíhání případů kybernetické kriminality
Vězení a probace
• Dodatečné náklady spojené s probací • Uvěznění pachatelů kybernetické kriminality
Reakce mimo systém trestní justice
• Hlášení/dokumentování případů • Právní výdaje, PR a podobné výdaje • Zvýšené/lépe vynaložené náklady na IT jako přímá reakce na viktimizaci • Školení/vzdělávání jako přímá reakce na viktimizaci • Změna poskytovatelů internetových služeb, poskytovatelů bezpečnostních opatření nebo produktů jako přímá reakce na viktimizaci • Snížení nákladů na výzkum a vývoj

Pracovní skupina zpočátku uvažovala, zda by bylo možné vyplnit rámec s použitím literatury, která byla již akademickou komunitou publikována a je uvedena v Kapitole 4. Záměrem bylo vyplnění rámce hodnotami převzatými z literatury, což by umožnilo identifikovat chybějící údaje. Odhady získané na základě rešerše odborné literatury však vesměs nebyly Pracovní skupinou shledány dostatečně spolehlivými či vhodnými pro to, aby mohly být použity k doplnění rámce ve vztahu k nákladům kybernetické kriminality v ekonomice UK. Jednalo se zejména nedostatky v těchto oblastech:

- metodologické otázky (např. nebyl měřen správný typ nákladů);
- nesrovnatelnost pramenící z rozdílů v měření nebo vyloučení/zahrnutí určitých typů kybernetické kriminality, jako například krádež duševního vlastnictví;
- nedostatečná transparentnost použité metody; a
- problémy s odhadem dopadu na britský systém trestní justice.

Takto vyplněný rámec by proto poskytoval jen nepřesný odhad celkového stavu.

Výsledný rámec prezentovaný v této zprávě (Tabulka 2 a 3) proto nejsou vyplněny a neobsahují žádné odhady. Jeho smyslem je identifikovat oblasti budoucího výzkumu s tím, že mohou být účelným nástrojem vizualizace nákladů spojených s kybernetickou kriminalitou v rámci ekonomiky UK. Cílem je podnítit další výzkum, který by začal naplňovat výzkumný rámec a napomohl tak získat více poznatků o nákladech souvisejících s touto specifickou oblastí kriminality.

V zájmu konzistentnosti přístupu Home Office k nákladům spojeným s kriminalitou by měly být hodnoty nákladů kybernetické kriminality uváděny jako ekonomické náklady UK na jeden incident. Takové hodnoty pak mohou být použity ve spojení se samostatnými odhady vztahujícími se k různým typům incidentů za rok. Spolu se spolehlivými odhady rámec navíc umožní sledování pokroku při shromažďování údajů v této oblasti pro doporučení budoucí strategie UK ve vztahu ke kyberkriminalitě. Vezmeme-li v úvahu dopady kybernetické kriminality v různých oblastech, výzkumný rámec rovněž dovolí konsolidaci informací a dat z existujících zdrojů v řadě oblastí, včetně (ale nejen) vlády, prosazování práva, organizací, podnikatelských subjektů a neziskových organizací.

Závěrem je nutno říci, že výzkumný rámec týkající se nákladů spojených s kybernetickou kriminalitou není míněn jako definitivní vyjádření toho, jak přesně by kybernetická kriminalita měla být měřena, ale spíše jako výchozí bod pomáhající ukázat, co je v této oblasti známo, a poskytnout návod, kterého by se mohli odborníci a agentury držet. Je důležité poznamenat, že některé náklady zahrnuté ve výzkumném rámci se objeví, i kdyby byla kybernetická kriminalita nulová (např. bezpečnostní prověřování zaměstnanců nebo dodavatelů); je třeba, aby v budoucích studiích výzkumníci vyčlenili/přičetli takové náklady kybernetické kriminalitě.

Příklad výzkumného rámce nákladů spojených s kybernetickou kriminalitou

Tabulka 3 ukazuje, jak může být pojat rámec nákladů spojených s kybernetickou kriminalitou ze strany těch, kdo se pokusí jej v budoucnu vyplnit. Ilustrace zdůrazňuje jeden sloupec z rámce vztahující se k malwaru.

Rámec zahrnuje ve sloupcích typy jednání rozdělené na trestné činy závislé na ICT a trestné činy usnadněné ICT. Ty jsou dále rozčleněné na čtyři odlišné ekonomické aktéry (malé a střední podniky, velké obchodní podniky, vládní subjekty a jednotlivé osoby). Řádky ukazují náklady kyberkriminality rozlišené jako náklady anticipace, náklady dopadu a náklady vynaložené v reakci na kyberkriminalitu. Dále jsou rozděleny na specifické náklady v jednotlivých kategoriích. Pro každou nákladovou položku umožňuje rámec vyplnění celkového odhadu pro danou kategorii (např. trestná činnost usnadněná ICT) nebo specifickou formu (např. odmítnutí služby nebo distribuované odmítnutí služby, DDoS). Čtenáři navíc mohou sledovat odhady nákladů ve vztahu k odlišným ekonomickým aktérům, kteří nesou náklady kyberkriminality. Slovníček klíčových slov použitých ve výzkumném rámci je uveden v Příloze 2.

Tabulka 3 - Příklady ilustrující výzkumný rámec nákladů spojených s kybernetickou kriminalitou

	Škodlivý software					
	Vládní entity	**LBE**	**SME**	**Osoby**	**Jiné**	**Celkově**
Náklady anticipace / prevence						
Technologie						
1. Software/produkty pro ochranu počítačové bezpečnosti (např. antivirus, záplatování)						
2. Zavedení/doplnění technologií						
Školení						
3. Školení/vzdělávání v oblasti kybernetické bezpečnosti						
4. Výcvik policejních vyšetřovatelů a důstojníků						
5. Školení soudního a právního personálu						
Bezpečnostní praktiky/chování						
6. Implementace zásad kybernetické bezpečnosti						
7. Vliv zvýšených bezpečnostních opatření na uživatele a obvyklé používání						
8. Výměna poskytovatelů internetových služeb (ISP), poskytovatelů bezpečnostních opatření nebo produktů za účelem zvýšení bezpečnosti						
9. Bezpečnostní prověření zaměstnanců a dodavatelů						
10. Sledování zabezpečení třetích stran						
11. Prověřování úvěrových záznamů /výsledků						
12. Vyhýbání se používání internetu a/nebo jiných technologií (mezi neuživateli)						
Vládní aktivity						
13. Příprava a tvorba nové legislativy						
14. Snaha vzdělávat veřejnost v nové legislativě						
15. Realizace národních kampaní na zvyšování povědomí/ochrany						
Jiné						
16. Správa pojištění kybernetických rizik						
17. Služby zajišťující ochranu spotřebitele a identity						
18. Obavy/strach z kybernetické kriminality						
19. Shromažďování statistických údajů o kybernetické kriminalitě						
Anticipace/prevence celkem						

	Škodlivý software					
	Vládní entity	LBE	SME	Osoby	Jiné	Celkově
Náklady dopadu útoku						
Náklady na řešení útoku						
1. Poškození zařízení/infrastruktury						
2. Výdaje na likvidaci následků						
3. Korigování úvěrových záznamů/ výsledků						
Finanční ztráty						
4. Narušení obchodní činnosti, včetně ztráty produkce						
5. Online krádež/podvod týkající se finančních zdrojů						
6. Ztracená hodnota DV/obchodně citlivých informací						
7. Poškození dobré pověsti nebo hodnoty obchodní značky						
8. Sporné transakce						
Jiné						
9. Emoční/fyzické újmy						
10. Služby na podporu obětí						
Dopad kybernetického útoku celkem						

Náklady vynaložené v reakci na útok						
Reakce systému trestní justice						
Prosazení práva						
1. Vyšetřování a vymáhání práva						
Soudy						
2. Soudní stíhání případů kybernetické kriminality						
Vězení a probace						
3. Dodatečné náklady spojené s probací						
4. Uvěznění pachatelů kybernetické kriminality						
Reakce systému trestní justice celkem						
Reakce mimo systém trestní justice						
5. Hlášení/dokumentování případů						

	Škodlivý software					
	Vládní entity	**LBE**	**SME**	**Osoby**	**Jiné**	**Celkově**
6. Právní výdaje, PR a podobné výdaje						
7. Zvýšené/lépe vynaložené náklady na IT jako přímá reakce na viktimizaci						
8. Školení/vzdělávání jako přímá reakce na viktimizaci						
9. Změna poskytovatelů internetových služeb, poskytovatelů bezpečnostních opatření nebo produktů jako přímá reakce na viktimizaci						
10. Snížení výdajů na výzkum a vývoj						
Reakce mimo systém trestní justice celkem						
Celkové náklady vynaložené v reakci na kybernetickou kriminalitu						
Celkově						

IV.

Souhrn poznatků vyplývajících z výzkumu uskutečněného Pracovní skupinou

Vedle vytvoření výzkumného rámce týkajícího se nákladů spojených s kybernetickou kriminalitou řešila Pracovní skupina řadu samostatných výzkumných projektů, a to s cílem zlepšit kvalitu dat potřebných pro pochopení nákladů spojených s kybernetickou kriminalitou a začít zaplňovat mezery ve znalostech. Tyto projekty byly řešeny akademickými pracovníky z řady univerzit a fakult. Tato kapitola poskytuje krátké shrnutí hlavních zjištění jednotlivých projektů; Příloha 4 odkazuje čtenáře na podrobnější zprávy, které byly publikovány.

1. Odhad rozšíření a finančních dopadů web defacementu v UK

Cílem studie provedené Dr. Maxem Kilgerem a Dr. Tomem Holtem bylo zhodnotit prevalenci, povahu a finanční dopad web defacementu na podnikatelské subjekty a jednotlivé osoby v UK. Kromě odhadu nákladů studie rovněž zkoumala, zda jednotlivé faktory pozorované v obsahu web defacementu mohou být použity k predikci nákladů spojených s těmito útoky.

Web defacement je jedna ze starších forem škodlivých online útoků, které zahrnují nahrazení hlavní webové stránky obrázky a obsahem podle útočníkova výběru. Ačkoli web defacement nemusí být tak škodlivý, jako nainstalování škodlivého softwaru nebo prolomení ochrany dat, přesto může být takový útok pro oběť nákladný, zejména když se jedná o nehmotné náklady spojené s poškozením dobré pověsti oběti.

V rámci studie byla učiněna řada odhadů finančních dopadů web defacementu s použitím vzorku 1250 případů nahlášených internetovým stránkám Zone-H. Zone-H je jedním z nejobsáhlejších archivů web defacementů a je prostorem, kde hackeři veřejně ohlašují/propagují webové stránky, které napadli.

Celkové náklady vynaložené vládou a napadenými průmyslovými cíli zmíněných 1250 případů web defacementu zaznamenaných v letech 2007-2015 jsou odhadovány na přibližně 1,6 milionu liber.

K interpretaci odhadů zahrnutých v tomto výzkumu bychom měli přistupovat obezřetně. Odhady byly podpořeny daty US Computer Security Institute, a i když jsou tato data považována za nejlepší a jediná dostupná, je s nimi spojena řada omezení. Existují rovněž omezení týkající se informací zahrnutých v souboru dat Zone-H a není úplně jasné, jak reprezentativní jsou případy v tomto souboru zahrnuté z hlediska web defacementu vůbec.

Provedený výzkum upozornil na obecný problém při odhadování nákladů spojených s kybernetickou kriminalitou vůbec – nedostatek vhodných primárních dat. Pro přesnější odhad nákladů tohoto a dalších typů kyberkriminality v UK by byl třeba další primární výzkum např. mezi podnikatelskými subjekty.

Studie rovněž naznačila, že má smysl vyvíjet modely web defacementu ze strany teprve se formujících škodlivých činitelů – za účelem identifikace, které z těchto aktivit mají největší potenciál působit ekonomické ztráty. To by mohlo umožnit zaměření pozornosti při prosazování práva a jiných zmírňujících zásahů na ty nejzávažnější útoky.

2. Odhady rozsahu a nákladů spojených s působením malwaru v rámci UK

Cílem studie provedené Dr. Tomem Holtem bylo prověřit rozsah a náklady spojené s infekcí malwarem, a to pomocí alternativního a méně užívaného zdroje informací, kterým byl Malware Domain List. Jde o objektivní otevřený zdroj informací poskytující seznam škodlivých softwarů, které byly identifikovány v prostředí webových serverů užívaných v UK, spolu s údaji o povaze infekce (např. bot[21] nebo exploit[22]).

Tato studie identifikovala 89 celkových infekcí, které byly zahrnuty v Malware Domain List v letech 2009 až 2014. Toto číslo je bezpochyby podhodnoceno, vzhledem k celkovému počtu infekcí, ke kterým došlo v tomto období, avšak nemáme jiné zdroje dat, které by nám umožnily učinit skutečný odhad. Není jasné, proč je číslo tak nízké, důvodem pravděpodobně může být nízká míra ohlašování těchto událostí nebo nízký počet infekcí na úrovni serveru. Proto by poznatky z tohoto výzkumu měly být interpretovány s nejvyšší opatrností a mělo by se uvážit, zda má do budoucna cenu využívat Malware Domain List jako samostatný zdroj informací.

Studie odhaduje, že identifikované infekce malwarem v období let 2009-2014 mohly způsobit společnostem podnikajícím v UK náklady zhruba ve výši 5,1 milionu liber. Přestože jednotkové náklady malwaru byly získány z nekvalitního zdroje, což může ovlivnit hladinu spolehlivosti tohoto odhadu, je důležité poznamenat, že jde o jeden z mála dostupných zdrojů informací. Pokud by byl v budoucnu k dispozici přesnější zdroj údajů, další primární výzkum (např. mezi podnikatelskými subjekty) by umožnil přesnější odhad nákladů spojených s tímto a dalšími typy kybernetické kriminality v UK.

3. Odhady výnosů a ztrát na ilegálních trzích

Studie provedená Dr. Tomem Holtem a Dr. Olgou Smirnovovou se dívá na náklady spojené s kybernetickou kriminalitou alternativním úhlem pohledu, neboť se zaměřuje na výši zisků pachatelů.[23] Jejím cílem proto bylo prozkoumat rozsah dat a služeb spojených s kybernetickou kriminalitou, které přímo ovlivňují nebo cílí na občany, průmysl nebo vládu UK, a které jsou prodávány na nezákonných online trzích, a to jak na open webu, tak v dark webu.

Tento projekt se rovněž zaměřil na odhad příjmů aktérů na nelegálním trhu (např. tržní aktéři kupující a prodávající data) a na náklady potenciálních obětí, založené na prevalenci malwaru, hackingu a osobních údajů obchodovaných online. Představa byla taková, že takto odlišný přístup k nákladům spojeným s kybernetickou kriminalitou doplní existující výzkum a pomůže vytvořit celistvější obrázek různých nákladů s ní spojených.

21 Nástroj, který vykonává na internetu předem určenou činnost (tzv. skript – série příkazů – pozn. překl.).

22 Software spuštěný na webovém serveru, který identifikuje slabiny v klientských zařízeních komunikujících s daným serverem.

23 Zisky/ztráty pachatelů nebyly v předchozích výzkumech nákladů kriminality prováděných ze strany Home Office zohledněny. Byly nicméně zahrnuty do tohoto pracovního plánu, aby se ukázalo, jak může lepší porozumění takovýmto odhadům zlepšit i pochopení různých nákladů spojených s kybernetickou kriminalitou vůbec.

Na základě vzorku 18 fór a 15 obchodů umístěných na open webu a Toru[24] poskytla studie metodologii pro výpočet množství potenciálních transakcí, které uskutečňují prodávající, a potenciálních zisků aktérů prodávajících a kupujících data na těchto trzích.

Na základě uvedeného vzorku studie odhadla, že prodávající, kteří nabízejí hromadně data týkající se kreditních a debetních karet, CVV data (zahrnující čísla kreditních karet a samotné CVV) a eBay a PayPal účty, mohou vydělat zhruba 4 000 až 16 000 liber při minimální ceně a mezi 89 000 a 355 000 librami při mediánové ceně. Co se týká vzorku zahrnujícího dark web, studie odhaduje, že prodávající vydělali částku mezi 13 000 a 54 000 librami při uplatnění minimální ceny a 24 000 až 95 000 liber při mediánové ceně. Zisky prodávajících se lišily podle typu, ceny a množství prodaných dat. To vytváří podstatné rozdíly ve výnosech, ale ukazuje se, že prodávající mohou generovat vysoké příjmy i při použití minimální ceny a největší zisky mohou generovat zejména při hromadném prodeji.

Zisky aktérů kupujících data byly podobně variabilní. Studie odhaduje, že jejich výnosy z odcizených finančních dat se podle vzorků transakcí na open webu i dark webu pohybovaly mezi 6,1 milionu a 25,2 milionu liber, a to v závislosti na tom, kolik účtů bylo aktivních při pořizování v dávkách souborů dat o 50 účtech. Studie zjistila, že navzdory nízké pravděpodobnosti použitelných dat nebo úspěšných transakcí mohou kupující získat potenciálně miliony liber. Výnosy kupujících jsou odhadnuty na stovky tisíc, i když se návratnost počítá z menšího množství použitelných dat.

Odhady odvozené z těchto modelů jsou předběžné a musí být interpretovány s opatrností. Pravděpodobně podhodnocují celkový počet provedených transakcí a nezahrnují náklady na práci, čas a jiné nesledované náklady na straně prodávajících/kupujících. Výsledky nicméně demonstrují, že prodej a nákup dat je výnosným podnikem a může se podílet na dlouhodobé existenci trhů zahrnutých v uvedeném vzorku.

4. Poškození dobré pověsti podnikatelských subjektů jako důsledek kybernetické kriminality

Cílem této studie provedené výzkumnou agenturou Kantar Public (dříve známou jako TNS BMRB) byl primární kvalitativní výzkum, který by podpořil navržení kvantitativních měření tak, aby mohla být replikována a použita v budoucích studiích vyhodnocujících dopad kybernetické kriminality na dobrou pověst podnikatelských subjektů.

Kvalitativní terénní výzkum zahrnoval hloubkové rozhovory s podnikatelskými subjekty, z nichž některé měly zkušenost s kybernetickou kriminalitou, a jiné nikoliv. Subjekty zahrnuté v této počáteční kvalitativní části výzkumu představovaly směsici malých a středních podniků, jakož i velké podniky. Po těchto hloubkových rozhovorech následovaly fokusní skupiny zahrnující zástupce veřejnosti. Ačkoliv takto koncipovaný výzkumu neumožňuje generalizovat získané poznatky na celou populaci UK, skýtá výzkumníkům poznatky využitelné při navrhování a testování kvantitativních měření dobré pověsti podnikatelských subjektů.

24 Internetový prohlížeč, který umožňuje anonymní přístup na web (včetně dark webu).

Výzkum odhalil, že jak pro veřejnost, tak pro podnikatelské subjekty je obtížné „dobrou pověst" definovat, natož doporučit vhodný způsob měření její změny po kybernetickém útoku. Klíčové zjištění výzkumu mezi podnikatelskými subjekty bylo, že ačkoliv si dokázaly představit metodu odhadu finančního dopadu poškození dobré pověsti, nemyslely si, že by ji aktivně využívaly, aniž by došlo k velmi závažnému incidentu. Dotazovaní to vysvětlovali tak, že pokud by takové měření bylo třeba, bylo by nutné získat informace od různých jednotlivých skupin v rámci jejich společnosti – zejména od IT a marketingového oddělení. Účastníci navíc poznamenali, že aktuální kalkulace by byly extrémně citlivé a pravděpodobně by byly dostupné jen na úrovni správní rady. Tato skutečnost bude mít vliv na dostupnost potřebných informací o tomto druhu dopadu pro potřeby budoucích výzkumů.

Klíčové zjištění výzkumu mezi veřejností bylo, že kybernetické útoky nemusí vést ke změně společností nebo providerů. Velký význam byl přikládán tomu, jak se podnikatelské subjekty vypořádávají s chybami a omyly. „Dobrá" pověst nebyla spojena s neomylností; skutečnost, že k pochybením dochází, účastníci promíjeli. Očekávali však, že pokud dojde k problémům, podnikatelské subjekty přijmou zodpovědnost, rychle nabídnou řešení a se zákazníky budou jednat s respektem – domnívali se, že při druhém útoku by již byli méně shovívaví. Tato zjištění naznačují určité potenciální praktické vodítko pro podnikatelské subjekty, jak nejlépe reagovat nebo zmírnit dopad kybernetického útoku ve vztahu k dobré pověsti své společnosti. Tyto poznatky by stály za další testování a rozvinutí.

Po dokončení kvalitativního terénního výzkumu se studie zaměřila na vytvoření souboru kvantitativních nástrojů umožňujících hodnotit dopad kybernetické kriminality na dobrou pověst podnikatelských subjektů. Z diskusí s respondenty kvalitativního výzkumu bylo zřejmé, že prosté měření poškození dobré pověsti založené pouze na posouzení podnikatelských subjektů bude pravděpodobně velmi subjektivní a poskytne pouze odhady s velkým rozptylem. S ohledem na to studie uzavírá, že budoucí výzkum by měl k výpočtu používat řadu zdrojů umožňujících tak komplexnější a spolehlivější měření. Tyto zdroje by měly zahrnovat následující:

- **Studie událostí** – kvantifikuje poškození dobré pověsti s použitím ceny akcií coby jejího měřítka.
- **Sledování reputace** – ve velkých firmách zaměřených na velké množství zákazníků může být sledování reputace použito k porozumění dopadu kybernetické kriminality na dobrou pověst.
- **Analýza sociálních médií** – vytvořením souboru metrik může být provedena analýza hodnotící reakci sociálních médií prostřednictvím těchto nástrojů.
- **Shromažďování dat z výzkumů podnikatelských subjektů** – shromažďováním podrobností o povaze útoku a jeho dopadu na podnikání budou moci výzkumníci identifikovat závažné a méně závažné útoky.

Rozsah nebo komplexnost odhadu, který se má provést, může záviset na jeho potřebě ze strany podnikatelských subjektů. Předpokládalo se, že by tyto subjekty mohly učinit přinejmenším velmi jednoduché posouzení pravděpodobnosti poškození dobré pověsti kyberútokem na základě několika klíčových rizikových faktorů identifikovaných výzkumem:

- viditelnost útoku pro zákazníky a klíčové zainteresované osoby;
- přímé dopady na zákazníky/zainteresované osoby;

- zabezpečení dat co by primární reakce vůči klientům;
- opakované incidenty;
- kritické načasování útoku; a
- způsob vypořádání se s útokem a reakce na něj.

Takové posouzení by mohlo sloužit rovněž k uvážlivější reakci na incident a pro vypracování plánů, jak se bránit budoucím kybernetickým útokům.

S ohledem na uvedené závěry výzkumný tým vypracoval řadu výzkumných otázek pro shromažďování dat v budoucích výzkumech týkajících se podnikatelské sféry. Zmíněné otázky jsou prezentovány v Příloze 3.

5. Pochopení šíře, trendů a měření trestné činnosti závislé na použití ICT

Cílem studie provedené Davidem Emmem, prof. Stevem Furnellem a Dr. Marií Papadaki bylo lépe pochopit rozsah měření používaných pro odhad prevalence a incidence trestné činnosti závislé na ICT, včetně:

- virů a jiného malwaru;
- odmítnutí služby (DoS) nebo distribuovaného odmítnutí služby (DDoS); a
- hackingu.

Taková měření jsou používána k porovnání rozsahu hrozby, kterou každá z těchto podob kybernetické kriminality představuje z hlediska objemu a frekventovanosti dané hrozby. Lepší předporozumění v tomto směru je nápomocné při budování výchozí důkazní základny pro náklady spojené s kybernetickou kriminalitou.

V rámci zmíněného výzkumu byla provedena rešerše různých publikovaných zdrojů (např. od poskytovatelů zabezpečení, bezpečnostních studií a zpráv o hrozbách) za účelem určení povahy a kvality hlavních měření vztahujících se (v roce 2016) ke kriminalitě závislé na ICT.

Rešerše ukázala, že rozdíly mezi stávajícími používanými nástroji a přístupy neposkytují pro kvantifikaci kriminality závislé na ICT jednoznačný mechanismus. Stávající kritéria mohou při sledování trendů postrádat hloubku, srovnatelnost a ucelenost. Navíc mohou být data zkreslena v závislosti na geografickém umístění a proto, že některá čísla jsou založena pouze na informacích získaných ze zabezpečených zařízení a reflektují jen útoky detekované poskytovateli zabezpečení.

Studie zjistila, že by bylo nerozumné a potenciálně zavádějící vybrat si izolovaně jediné měření či zprávu a považovat je za nejpřesnější odhad. Odlišná měření poskytují odlišné úrovně vhledu – nelze říci, že jsou to špatná měření, ale výběr nástrojů závisí na tom, co přesně je posuzováno. Jednoduché měření objemu dává mnoho různých validních možností.

Rešerše nicméně zjistila, že pro pochopení hrozeb je zjevně třeba dospět ke konzistentnějšímu slovníku, terminologii a obecnému rámci. To však může přinést užitek pouze při široké a dostatečně silné podpoře na to, aby zajistila všeobecné přijetí a používání. Předchozí pokusy v tomto směru nebyly úspěšné.

Výzkum též vzal v úvahu odpovědi zkušených bezpečnostních expertů, kteří mají přístup k ohroženým datům. I když bezpečnostní experti navrhli řadu nástrojů, které lze použít ke sběru dat, která by mohla ukázat rozsah a trendy, sami nebyli přesvědčeni, že má cenu to udělat. Obecně se věří, že je důležitější porozumět důsledkům útoků, ale tento názor by stanovil jiný okruh otázek z hlediska dostupnosti dat.

Studie došla k závěru, že měření škály, rozsahu a frekvence trestné činnosti závislé na ICT samo o sobě nestačí. Na určité úrovni je třeba provázat je se závažností, dopadem a náklady incidentu. Vysoká čísla publikovaná v globálních nebo regionálních zprávách mají velmi dramatický účinek, ale pro podnikatelské subjekty nejsou nutně významná. Ty potřebují porozumět dopadům na jejich podnikání a skutečné náklady budou velmi záležet na dopadu na konkrétní napadenou organizaci.

6. Zkoumání následků strachu z kybernetické kriminality

Cílem této studie prof. Matthewa Williamse bylo celoevropské srovnání strachu z kybernetické kriminality (včetně ekonomické kyberkriminality a kyberkriminality spojené s obsahem) a vyvarovávání se jí. Analýzu umožnila kombinace tří průzkumů Eurobarometr (Eurobarometer Cybersecurity Survey, 2012, 2013, 2014).

V analýze byla zahrnuta čtyři přímá měření strachu z kybernetické kriminality obsažená v rámci Eurobarometru:
- obava z online krádeže identity;
- obava z online podvodu při nakupování;
- obava z vystavení nemravnému zobrazení dětí; a
- obava z vystavení materiálům podporujícím rasovou nenávist nebo náboženský extremismus.

Uvedené faktory byly spojeny do dvou hlavních složek:
- obava z ekonomické kyberkriminality (strach z online krádeže identity a online podvodu při nakupování); a
- obava z kyberkriminality související s obsahem (obava z vystavení nemravnému zobrazení dětí a z vystavení rasové nebo náboženské cyberhate[25]).

Analýza vyhýbání se kybernetické kriminalitě zahrnovala v průzkumech dvě otázky: vyhýbání se online bankovnictví a online nakupování.

Celkově studie zjistila, že větší obavy panují ohledně ekonomické kyberkriminality než z kyberkriminality spojené s obsahem. Velká Británie se umístila z hlediska míry strachu z ekonomické kyberkriminality v rámci Evropy na šestém místě, za Českou republikou,

25 Projev nesnášenlivosti online – pozn. překl.

Litvou, Španělskem, Lotyšskem a Francií. Irsko se objevilo na sedmém místě. Bylo překvapivé, že na spodních příčkách vykazujících nejmenší strach z ekonomické kyberkriminality se objevila skupina severských zemí (Švédsko, Dánsko a Finsko) a Nizozemí, spolu s Rumunskem, Maďarskem a Slovinskem.

Studie rovněž zjistila, že Velká Británie se v rámci Evropy umístila na čtvrtém místě z hlediska obav z kyberkriminality spojené s obsahem, za Českou republikou, Španělskem a Litvou. Irsko a Francie se objevily na šestém a sedmém místě. Podobně jako u ekonomické kybernetické kriminality, skupina skandinávských zemí (Švédsko, Dánsko a Finsko) spolu s Nizozemím obsadily nejnižší příčky, neboť vykazovaly nejmenší obavy z kyberkriminality spojené s obsahem.

Velká Británie skončila pátá z hlediska online vyhýbání se, za Švédskem, Lucemburskem, Belgií a Nizozemím. Francie a Irsko se objevily na šestém a devátém místě. Východoevropské země (Bulharsko, Lotyšsko, Polsko, Slovensko, Litva a Estonsko) byly z hlediska vyhýbání se na nejnižších příčkách.

Víceúrovňová regresní analýza ukázala, že zkušenost s kyberkriminalitou spojenou s obsahem byla nejsilnějším prediktorem vyhýbání se, zatímco zkušenost s ekonomickou kyberkriminalitou byla až třetím nejvýznamnějším faktorem. Statisticky signifikantně pravděpodobnější k zaujmutí vyhýbajícího se postoje byly ženy, senioři a ekonomicky znevýhodnění lidé. Oběti kybernetické kriminality, ženy, rodiče, ekonomicky znevýhodněné osoby a osoby žijící ve venkovských oblastech se kybernetické kriminality obávali statisticky signifikantně více. Významným prediktivním faktorem obav z kybernetické kriminality byl také věk. V rámci Evropy dosahovaly obavy vrcholu ve věku 38 let v souvislosti s ekonomickou kyberkriminalitou (45 let u mužů a 31 u žen) a ve věku 43 let u kyberkriminality spojené s obsahem (47 let u mužů a 37 u žen). Ve Velké Británii panují nejvyšší obavy z ekonomické kyberkriminality ve věku 46 let a z kyberkriminality spojené s obsahem ve věku 47 let.

Studie je zakončena úvahou nad vhodností odhadování peněžních nákladů kybernetické kriminality pro tvůrce politiky a justici. Zmiňuje, že ačkoliv některé metody, jako je zjišťování stínové ceny (oceňování používající náhradní hodnoty určené pravděpodobnými náklady příležitosti na získání zboží nebo komodity), byly aplikovány na zjišťování obav z offline kriminality, nemohou být použity pro kybernetickou kriminalitu, protože taková data v současnosti nejsou dostupná. V blízké budoucnosti bude nicméně možné provést peněžní odhad nákladů ve vztahu ke kyberkriminalitě zaměřené na jednotlivce i podnikatelské subjekty, jakmile budou k dispozici soubory dat (např. CSEW).

v.

Diskuse a směřování dalšího výzkumu

Tato zpráva zdůrazňuje řadu klíčových skutečností vyplývajících ze studia existující literatury a napomáhá zvýšit povědomí o klíčových faktorech pro odhadování nákladů spojených s kybernetickou kriminalitou. Příklady nových odhadů nákladů jsou následující.

- Jedna ze studií odhadla, že celkové náklady spojené s 1 250 případy web defacementu zaměřeného na vládní a průmyslové cíle, ke kterým došlo v letech 2007 až 2015, dosáhly 1,6 milionu liber, s průměrnými náklady na jednotlivý defacement přibližně ve výši 1 200 liber.[26]
- Studie zaměřená na infekce malwarem oznámené na úrovni serverů v rámci UK ukázala, že odhadované náklady pro společnosti působící na území UK spojené s celkovým počtem 89 infekcí oznámených prostřednictvím Malware Domain List v letech 2009 až 2014 činily 5,1 milionu liber, s průměrnými náklady na jednu infekci přesahujícími 57 000 liber.[27]
- Výzkum založený na vzorku transakcí za určitou dobu zjistil, že ti, co zakoupili na open webu a dark webu odcizená finanční data, zřejmě získali jejich využitím mezi 6,1 a 25,2 miliony liber v závislosti na tom, kolik z účtů pořizovaných v souborech po 50 bylo aktivních.
- Výzkum zabývající se výdělky prodejců odcizených finančních dat dospěl k novému mediánovému odhadu mezi 89 000 a 355 000 librami. V rámci vzorku v dark webu prodejci vydělali při použití mediánové ceny mezi 24 000 a 95 000 liber.

Je třeba poznamenat, že uvedené poznatky mají svá omezení. Často jsou založeny na malých vzorcích dostupných dat a pravděpodobně představují pouze malou část celkových nákladů. Jsou rovněž odkázané na kvalitu výchozích zdrojů dat – studie odhalily zřetelný nedostatek kvalitních primárních dat, které by byly k dispozici pro odhady jednotkových nákladů. Studie tak byly odkázané na těch několik dostupných zdrojů, o kterých se vědělo, že mají řadu omezení.

Přesto však uvedená zjištění pomohla prozkoumat a pochopit hodnotu alternativních zdrojů dat pro získání dalších znalostí v této oblasti. Jedna studie též poskytuje alternativní pohled na náklady – z perspektivy pachatele.

Vedle nového porozumění některým nákladům spojeným s kybernetickou kriminalitou identifikoval kvalitativní výzkum, součást projektu zkoumajícího způsoby měření dopadu kyberkriminality na dobrou pověst subjektů byznysu, řadu možných postupů, které mohou aplikovat podnikatelské subjekty, aby lépe pochopily dopad kyberútoku na svou reputaci. Stejný výzkum též zjistil, že veřejnost přisuzuje význam tomu, jak se podnikatelské subjekty vypořádávají s chybami a omyly. Respondenti hovořili o tom, jak pomíjí skutečnost, že k chybám došlo, ale očekávají, že dojde-li k problémům, podnikatelské subjekty za ně převezmou odpovědnost, rychle nabídnou řešení a budou jednat se zákazníky s úctou – respondenti však připustili, že v případě dalšího útoku by již byli méně shovívaví. Tento typ poznatků by mohl podnikatelským subjektům pomoci při oznamování své reakce spotřebitelům/klientům. Klíčové aspekty dobré reakce z pohledu dotazovaných spotřebitelů a podnikatelských subjektů zahrnovaly:

26 Je ovšem třeba poznamenat, že náklady se rok od roku liší, a nejde tedy o statické číslo.

27 Je ovšem třeba poznamenat, že jednotlivé náklady jsou ovlivněny typem malwaru a v různých letech se liší, což znamená, že přesné náklady na infekci se mohou od této průměrné hodnoty odlišovat.

- rychlá, poctivá a informovaná reakce;
- přímá komunikace se zákazníky společnosti (nikoli zprostředkovaná, přes média);
- kvalitní zákaznický servis reagující na dotazy následující po incidentu, zaměstnanci zákaznického servisu by měli např. poskytovat konzistentní a erudované rady týkající se incidentu, měli by uklidňovat a být vůči dotazům zákazníků vnímaví; a
- je-li to nezbytné, poskytnutí náhrady nebo kompenzace ztrát a/nebo nepříjemností.

S ohledem na to, jaký význam respondenti připisovali řešení incidentu a reakci na něj, bylo pozoruhodné, že dotazované podnikatelské subjekty neměly žádný plán, jak na takový útok reagovat. Vyšlo najevo, že by tyto subjekty mohly být aktivnější a samy se předem připravit na případ takového útoku, spíše než jen pasivně čekat, až se „bouře přežene".

Celkově pracovní program napomohl lépe porozumět tomu, jak by mohli v budoucnu výzkumníci postupovat při odhadování celkových nákladů kyberkriminality nebo při odhadování jejich rozmanitých aspektů. Tato zpráva se sice nepokouší dospět k celkovému odhadu nákladů spojených s kybernetickou kriminalitou, avšak formulace jeho rámce (viz tabulka 2) výzkumné komunitě pomáhá se tomuto cíli přiblížit. Zmíněný rámec má za cíl poskytnout výzkumným pracovníkům jasnější směr, kam napřít budoucí výzkum, aby patřičně zaplnil četné mezery v poznání.

Rešerše literatury, která byla provedena v rámci tohoto pracovního programu, odhalila řadu problémů a omezení týkajících se odhadů nákladů dostupných v době výzkumného programu. Výrazným omezením byl fakt, že mnoho studií stavělo své odhady na nekvalitních výzkumných datech co do škály a nákladů kyberkriminality. To sice ovlivnilo předchozí výzkum, do budoucna však můžeme být optimističtí, co se týče nových studií a dat pro dosahování lepších odhadů.

V roce 2016 publikovalo Ministerstvo kultury, médií a sportu výsledky nového výzkumu podnikatelských subjektů - Cyber Security Breaches Survey (DCMS, 2016).[28] Studie prezentovala řadu užitečných poznatků, včetně odhadu průměrných nákladů spojených s prolomením ochrany u velkých obchodních podniků ve výši 36 500 liber a nejnákladnějším prolomením ochrany vyčísleným na 3 miliony liber. Tento výzkum je inovovanou verzí studie prováděné v předchozích letech Ministerstvem obchodu, inovací a dovedností (BIS) a soukromým podnikatelským subjektem Price Waterhouse Cooper a v současné době představuje nejspolehlivější použitý metodologický přístup. Použita byla metoda náhodného výběru ve spojení s telefonním dotazováním 1 008 britských podnikatelských subjektů, přičemž data byla statisticky reprezentativní pro tyto subjekty co do jejich velikosti a hospodářského sektoru. Poznatky této studie poskytují výzkumníkům cennou příležitost lépe porozumět důsledkům kybernetického prolomení ochrany v UK s perspektivou budoucí identifikace trendů prolamování, neboť umožňuje pochopit, jak se tato aktivita mění v čase.

Podobně byly zlepšeny odhady prevalence kybernetické kriminality terénním testováním otázek, které měly být obsaženy v Crime Survey for England and Wales prováděné ze

28 Nejnovější verze byla v době tohoto výzkumu publikována v dubnu 2017 a je přístupná zde: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2017.

strany Office for National Statistics (ONS, 2015). Po doplnění nových otázek do výzkumu publikovala ONS (2017) experimentální data ukazující, že v období od začátku ledna do konce září roku 2016 bylo v Anglii a Walesu spácháno zhruba 3,6 milionu podvodů a 2 miliony zneužití počítačů.[29] Experimentální data ukázala, že 61 % podvodů vedlo k finanční ztrátě, a z těchto případů jich 23 % znamenalo ztrátu větší než 500 liber. Při práci Pracovní skupiny tato data bohužel nebyla k dispozici, a proto nemohla být použita. Přesto nabízí počáteční analýza dat zachycených díky výše uvedeným otázkám větší porozumění rozsahu kybernetické kriminality (*tamtéž*) a pravděpodobně bude velmi přínosná pro orgány činné v trestním řízení a tvůrce politiky při zajišťování optimální alokace zdrojů pro boj s kyberkriminalitou.

I jiné nedávné studie nabízejí příležitosti k dalšímu prozkoumání. Například Commercial Victimisation Survey (CVS) prováděný ze strany Home Office nadále zveřejňuje použitelné údaje o kybernetické kriminalitě ve specifických sektorech na úrovni výchozích předpokladů. Výzkum publikovaný Bosslerem, Holtem a Burrussem (Bossler, Holt and Burruss, 2016) provedený v řadách policie a bezpečnostních složek UK (důstojníci, konstáblové a seržanti) studoval jejich vnímání kybernetické kriminality a zkušenosti se zajišťováním kybernetické bezpečnosti. Otázky směřovaly na čas strávený řešením různých případů kybernetické kriminality a mohou být použity k další výzkumné práci týkající se nákladů prosazování práva v oblasti kybernetické kriminality – v současnosti velká mezera v údajích výzkumného rámce.

Výzkumy, které používají spolehlivé metodologické přístupy, tzn. zahrnují metody náhodného výběru, a které dokáží pomoci při patřičném vyplňování klíčových mezer výzkumného rámce nákladů spojených s kybernetickou kriminalitou, mají potenciál rozvinout porozumění této oblasti. Je však velmi důležité, aby ti, kdo se snaží odhadovat náklady, vzali v úvahu, jak byl výběr učiněn a zda je z hlediska zájmové populace vskutku reprezentativní.

Kromě pokroku ve výzkumu jsou zde i různé jiné příležitosti k prohloubení podkladů k nákladům kyberkriminality. Tato zpráva dochází k řadě doporučení, jak provádět budoucí výzkum.

- **Výzkumníci, kteří navrhují budoucí studie týkající se nákladů spojených s kybernetickou kriminalitou, by měli: metodicky přistoupit ke svému výzkumu s využitím výzkumného rámce uvedeného v této zprávě; identifikovat mezery ve výzkumném rámci nákladů kyberkriminality; a formulovat otázky pro výzkum tak, aby mohly tyto mezery vyplnit**. V zájmu srovnatelnosti výsledků by se měli výzkumníci zaměřit na ekonomické náklady kyberkriminality v UK připadající na jeden incident a na samostatný odhad počtu těchto incidentů za rok. Odhad nákladů na jednu událost pak může být vynásoben odhadem prevalence těchto útoků a výsledné hodnoty sumarizovány. Výhledově to posune širší vědeckou komunitu k lepšímu porozumění celkovým nákladům kyberkriminality.

29 Nejnovější experimentální data ONS byla publikována v říjnu 2017 a jsou přístupná zde: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/june2017.

- **Budoucí výzkum by se měl zaměřit na nejvýznamnější mezery ve výzkumném rámci nákladů kyberkriminality.** Rešerše literatury např. nerozlišovala složky zahrnující hacking/průnik do počítače; předchozí výzkum rovněž nevzal v úvahu náklady spojené s prosazováním práva. Znatelnou mezeru a prioritu pro další výzkum představují zejména náklady spojené s prosazováním práva, a to s ohledem na úskalí odrazování a stíhání pachatelů v online prostředí. Naopak nepřiměřeně více se předchozí výzkum zaměřil na náklady vynaložené podnikatelskými subjekty a na kriminalitu usnadněnou ICT (zejména podvody). Budoucí studie by se měly více zaměřit na náklady kyberkriminality vynaložené ze strany jednotlivců a také vzít v úvahu celou škálu kybernetických trestných činů, včetně kriminality závislé na ICT. Pro zvýšení celkové úrovně znalostí týkajících se nákladů kyberkriminality by bylo užitečné zaměřit budoucí studie na tyto zjištěné nedostatky a na zlepšení dosud provedených odhadů.

- **Budoucí studie by měly blíže prozkoumat náklady a zisky pachatelů kybernetické kriminality.** Poznatky prezentované v této zprávě naznačují, že výzkum v této specifické oblasti by mohl být velmi přínosný pro tvůrce politiky. To bude zřejmě hrát významnou roli především v kontextu nové *National Cyber Security Strategy*[30] (HM Government, 2016), která zdůrazňuje význam zvyšování nákladů a snižování zisků pachatelů kybernetických trestných činů a přijímání opatření kladoucích kyberkriminalitě překážky. Budoucí výzkum v této oblasti by měl usilovat o podrobnější pochopení těchto nákladů a uvážit, jak nejlépe hodnotit dopady jakýchkoliv budoucích intervencí.

- **Budoucí studie by měly prověřit nástroje prezentované v Příloze 3 této zprávy zkoumáním finančních dopadů kybernetických útoků na hodnotu dobré pověsti podnikatelských subjektů.** Je třeba zmínit, že primární výzkum provedený za účelem vývoje těchto pokusných nástrojů doporučuje, aby v zájmu přesných a spolehlivých výsledků jakýkoliv výzkum, který je používá, zahrnul mnoho různých zástupců z řad subjektů byznysu.

- **V rámci nejlepšího možného využití dostupných dat o nákladech by měla být provedena hlubší analýza souboru dat Action Fraud.** Ačkoliv zpráva vytvořená pro Policii londýnské City určitým způsobem dostupná data analyzovala, je možné je ještě dále využít, protože kvalita těchto dat a oznamování se postupně zlepšují.

- **Budoucí výzkum by měl podrobněji zvážit, jak odhadovat peněžní náklady spojené se strachem z kybernetické kriminality.** Jakmile budou výzkumníkům k dispozici nová data, měla by být k odhadu peněžních nákladů spojených se strachem z kyberkriminality ze strany domácího obyvatelstva použita metoda stínových nákladů.

- **Budoucí studie by měly při odhadování nákladů spojených s kybernetickou kriminalitou používat stále spolehlivější výzkumná data. Například měření kybernetické kriminality CSEW a výzkum DCMS Cyber Security Breaches Survey.** Aplikace těchto stále spolehlivějších dat ve výzkumném rámci nákladů kyberkriminality prezentovaném v této zprávě by měla umožnit výzkumníkům vytvářet konzistentní a spolehlivé odhady nákladů, které nejlépe využijí dostupné informace.

30 Národní strategie pro kybernetickou bezpečnost – pozn. překl.

Literatura

Anderson, R., Barton, C., Bohme, R., Clayton, R., van Eeten, M. J. G., Levi, M., Moore, T. and Savage, S. (2012) Measuring the cost of cyber crime. Dostupné na: http://www.econinfosec.org/archive/weis2012/papers/Anderson_WEIS2012.pdf (2016-12-01).

Bossler, A. M., Holt, T. J. and Burruss, G (2016) *Examining UK constables' perceptions of cyber crime*. Prezentace na výročním zasedání American Society of Criminology, New Orleans, LA.

British Retail Consortium (2015) *BRC Retail Crime Survey 2014*. Dostupné na: http://www.soloprotect.com/uk/Data/Lone_Downloads/BRCRetailCrimeSurvey2014.pdf (2016-12-01).

Centre for Economics and Business Research (2015) *The business and economic consequences of inadequate cybersecurity*. Vcybersecurityf Veracode. Dostupnlena: https://info.veracode.com/analyst-report-cebr-business-and-economic- consequences-of--inadequate-cybersecurity.html (2016-12-01).

Cifas (2014) *Fraudscape: UK fraud trends*. Dostupné na: http://www.cifas.org.uk/secure/contentPORT/uploads/documents/External%20%20Fraudscape%20main%20report%20for%20website.pdf (2016-12-01).

City of London Police (2015) *The implications of economic cyber crime for policing*. Dostupné na: https://www.cityoflondon.gov.uk/business/economic-research-and- information/research-publications/Documents/Research-2015/Economic-Cybercrime- FullReport.pdf (2016-12-01).

DCMS (2016) *Cyber Security Breaches Survey. Main Report*. London: Department for Culture Media and Sport. Dostupné na: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/521465/Cybe r_Security_Breaches_Survey_2016_main_report_FINAL.pdf (2016-12-01).

Detica (2011) *The cost of cyber crime*. Dostupnlena: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the- cost-of-cyber-crime-full-report.pdf (2016-12-01).

Financial Fraud Action UK (2015) *Fraud the Facts 2015. The definitive overview of payment industry fraud and measures to prevent it*.

Florencio, D. and Herley, C. (2011) 'Sex, lies, and cyber-crime surveys'. In *Proceedings (online) of the Workshop on Economics of Information Security*. Microsoft Research. Dostupné na: http://research.microsoft.com/pubs/149886/SexliesandCyber crimeSurveys.pdf (2016-12-01).

Gee, J. and Button, M. (2015) *Countering fraud for competitive advantage: How UK FTSE listed companies can reduce the cost of fraud and maximize profitability*. PFK Littlejohn LLP. Dostupné na: https://www.accountant.nl/contentassets/40dd3944bac9446
f9bf8162f3fec650a/countering_f raud_for_competitive_advantage_2015.pdf (2016-12-01).

Government Statistical Service (2011) *National Statistician's Review of Crime Statistics: England and Wales, June 2011*. Dostupné na: https://www.statisticsauthority.gov.uk/archive/national-statistician/ns-reports--reviews-and- guidance/national-statistician--s-reports/national-statistician-s-review-of-crime-statistics.pdf (2016-12-01).

HM Government (2015) *2015 Information Security Breaches Survey*. Dostupné na: http://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-digital.pdf (2016-12-01).

HM Government (2016) *National Cyber Security Strategy 2016–2021*. Dostupné na: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf (2016-12-01).

HM Treasury (2003)[31] *The Green Book. Appraisal and Evaluation in Central Government*. Dostupné na: https://www.gov.uk/government/publications/the-green-book-appraisal--and- evaluation-in-central-governent (2016-12-01).
Home Affairs Select Committee (2013) *House of Commons Home Affairs Select Committee Report on E-crime*. Dostupné na: http://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/70/70.pdf (2016-12-01).
Home Office (2000) *The economic and social costs of crime*. London: Home Office. Dostupné na: http://webarchive.nationalarchives.gov.uk/20110218135832/rds.homeoffice.gov.uk/rds/pdfs/ hors217.pdf (2016-12-01).
Home Office (2013a) *Serious and Organised Crime Strategy*. London: Home Office. Dostupné na: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/248645/Serio us_and_Organised_Crime_Strategy.pdf (2016-12-01).
Home Office (2013 b) *Understanding organised crime: estimating the scale and the social and economic costs*. London: Home Office. Dostupné na: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246390/horr7 3.pdf (2016-12-01).
Home Office (2013c) *Cyber Crime: A Review of the Evidence*. London: Home Office. Dostupné na: https://www.gov.uk/government/publications/cyber-crime-a-review-of-the-evidence (2016-12-01).
Intellectual Property Office (2015) *IP Crime Report 2014/2015*. Dostupné na: https://www.gov.uk/government/publications/annual-ip-crime-report-2014-to-2015 (2016-12-01).
McAfee/Intel (2014) *Net losses: Estimating the global cost of cyber crime. Economic impact of cyber crime II*. Center for Strategic and International Studies. Dostupné na: http://www.mcafee.com/uk/resources/reports/rp-economic-impact-cybercrime2.pdf (2016-12-01).
National Crime Agency (2015) *National Strategic Assessment of Serious and Organized Crime 2015*. Dostupnlena: http://www.nationalcrimeagency.gov.uk/publications/560--national- strategic-assessment-of-serious-and-organised-crime-2015/file (2016-12-01).
National Fraud Authority (2013) *Annual Fraud Indicator*. Dostupné na: https://www.gov.uk/government/publications/annual-fraud-indicator--2 (2016-12-01).
Neustar (2015) *Neustar DDoS Attacks & Protection Report: EMEA* (Europe, the Middle East and Africa), March 2015. Dostupné na: https://ns- cdn.neustar.biz/creative_services/biz/neustar/www/resources/whitepapers/it- security/ddos/2015-uk-ddos-report.pdf (2016-12-01).
ONS (2015) *CSEW Fraud and Cyber-crime Development: Field Trial"*. Dostupné na: http://www.ons.gov.uk/ons/guide-method/method-quality/specific/crime-statistics- methodology/methodological-notes/methodological-note---csew-fraud-and-cyber-crime-development--field-trial---october-2015.pdf (2016-12-01).
ONS (2017) *Crime in England and Wales: Year ending Sept 2016*. Dostupné na: https://www.ons.gov.uk/releases/crimeinenglandandwalesyearendingsept2016 (2017-03-08).
Oxford Economics (2014) *Cyber-Attacks: Effects on UK Companies*. Zprmpa Centre for the Protection of National Infrastructure.
Ponemon Institute (2015) *2015 Cost of Cyber Crime Study: United Kingdom. Benchmark Study of UK Companies*. Dostupné na: http://www8.hp.com/us/en/software-solutions/ponemon-cyber-security-report/index.html (2016-12-01).
Ponemon Institute (2016) *Flipping the Economics of Attacks*. Dostupné na: http://www.ponemon.org/library/flipping-the-economics-of-attacks (2016-12-01).

31 Revidováno v roce 2011.

Symantec (2013) *2013 Norton Report – UK*. Dostupné na: http://www.symantec.com/content/en/us/about/presskits/b-norton-report-2013.en_uk.pdf (2016-12-01).
Symantec (2015) *ISTR 20* (Internet Security Report Threat).
ThreatMetrix (2015) *ThreatMetrix cyber crime report Q3.* Dostupné na: https://www.threatmetrix.com/wp-content/uploads/2015/11/ThreatMetrix-Cybercrime- Report-Q3-2015.pdf (2016-12-01).
Verizon (2015) *2015 Data Breach Investigations Report*. Dostupné na: http://www.verizonenterprise.com/DBIR/2015/ (2016-12-01).
Wall, D. S. (2007)[32] 'Policing cyber crimes: Situating the public police in networks of security within cyberspace', *Police Practice & Research: An International Journal*, 8 (2), pp. 183–205.
World Economic Forum (2014) *Global Information Technology Report 2014: Rewards and Risks of Big Data*. Dostupné na: http://www.weforum.org/reports/global-information-technology-report-2014 (2016-12-01).

32 Revidováno v květnu 2010 a únoru 2011.

Přílohy

Příloha 1 podává podrobnější přehled literatury k nákladům kyberkriminality.

Příloha 2 poskytuje slovník pojmů používaných ve výzkumném rámci nákladů kyberkriminality.

Příloha 3 prezentuje návrh kvantitativních nástrojů pro zjišťování hodnoty dobré pověsti subjektů byznysu za účelem posouzení dopadu kybernetických útoků na ni.

Příloha 4 odkazuje na podrobnější publikace vztahující se ke studiím, které pro tuto zprávu vybrala Pracovní skupina.

Příloha 5 uvádí výzkumné zadání Pracovní skupiny.

Příloha 6 předkládá seznam členů Pracovní skupiny.

Příloha 7 obsahuje slovníček nepřekládaných pojmů.

Příloha 1: Podrobnější přehled literatury k nákladům kyberkriminality

Aby bylo možno pochopit široký rozsah odhadů nákladů, k nimž dochází předchozí výzkumy, byla provedena online rešerše literatury vztahující se k odhadům nákladů kyberkriminality v UK, která byly publikována před 1. lednem 2016 a která sahá zpět až ke zprávě Detica (2011). Rešerše byla sestavena Dr. Adamem Bosslerem s podporou Home Office Analysis and Insight.

Detica, 2011

Protože bereme publikaci Detica (2011) jako výchozí bod, je třeba zmínit, že tam použitá definice kybernetické kriminality („nelegální aktivity pachatelů s cílem se obohatit, které využívají slabiny internetu a jiných elektronických systémů k nezákonnému přístupu nebo útoku na informace a služby používané ze strany občanů, podnikatelských subjektů a vlády") se liší od definice použité v tomto výzkumu a v ostatních podobných studiích, které dělí kybernetickou kriminalitu na usnadněnou ICT a závislou na ICT. To poukazuje na jeden z klíčových problémů identifikovaných rešerší – definice používané v této oblasti jsou natolik nekonzistentní, že uváděné odhady často nelze vůbec porovnávat. To se nevztahuje pouze na definici „kybernetické kriminality", ale rovněž na definice různých dalších konceptů, které ovlivňují celkové náklady spojené s kybernetickou kriminalitou.

Vezmeme-li v úvahu definici kybernetické kriminality použitou ve studii Detica, znamená to, že se zaměřujeme na:

- krádež identity a online podvody;
- krádež duševního vlastnictví, špionáž a vydírání; a
- fiskální podvody proti vládě.

Studie Detica zahrnula vypracování kauzálního modelu, který propojuje kybernetickou kriminalitu s jejím dopadem na ekonomiku UK. Přizpůsobila přístup odhadování nákladů kriminality použitý ve zprávě Home Office (2000), takže zahrnula:

- náklady anticipace;
- náklady dopadu;
- náklady vynaložené v reakci; a
- nepřímé náklady spojené s kybernetickou kriminalitou (např. poškození dobré pověsti, ztráta důvěry).

Studie Detica se zaměřila zejména na náklady dopadu spolu s některými náklady vynaloženými v reakci na kyberútok. Náklady spojené s anticipací kyberútoku nebyly blíže zkoumány. Kauzální model byl pak použit k rozdělení typů kybernetické kriminality do kategorií podle ekonomického dopadu. Mohl tak být použit k výpočtu rozsahu nákladů spojených s kybernetickou kriminalitou s použitím tříčíselného odhadu – nejhorší scénář, nejpravděpodobnější scénář a nejlepší scénář, ačkoli je třeba říci, že ne všechny tři typy odhadů se vždy ve zprávě vyskytovaly.[33] Zpráva došla k závěru, že podle nejpravděpodobnějšího scénáře činily odhadované náklady související s kybernetickou kriminalitou v UK 27 miliard liber, s poznámkou autorů, že odhad je pravděpodobně podhodnocený.

33 Např. ve vztahu ke ztrátě zákaznických dat zpráva uváděla pouze odhady nejlepšího a nejhoršího scénáře.

Celkový odhad nákladů vyčíslený na 27 miliard liber byl odvozený z řady jiných odhadů uvedených ve zprávě, z nichž ty nejvýznamnější uvádí následující tabulky.

Příklady nákladů uvedených ve zprávě Detica (2011):

Tabulka A1.1 Odhady nákladů spojených s kybernetickou kriminalitou pro občany UK

Náklady občanů	
Kybernetická kriminalita	**Ekonomické dopady**
Krádež identity	1,7 miliardy liber
Online podvod	1,4 miliardy liber
Screenware a falešný AV[34]	30 milionů liber

Zdroj: Detica (2011)

Tabulka A1.2: Odhady nákladů spojených s kybernetickou kriminalitou pro vládu UK

Náklady vlády	
Kybernetická kriminalita	**Ekonomické dopady**
Fiskální podvod	2,2 miliardy liber

Zdroj: Detica (2011)

Tabulka A1.3: Odhady nákladů spojených s kybernetickou kriminalitou pro subjekty byznysu v UK

Náklady subjektů byznysu	
Kybernetická kriminalita	**Ekonomické dopady**
Krádež DV – Letectví a obrana	0,4 miliardy liber
Krádež DV – Chemikálie	1,3 miliardy liber
Krádež DV – Elektronické a elektrické vybavení	1,7 miliardy liber
Krádež DV – Software a počítačové služby	1,6 miliardy liber
Krádež DV – Zdravotnictví, farmaceutika a biotechnologie	1,8 miliardy liber
Průmyslová špionáž – Letectví a obrana	1,2 miliardy liber
Průmyslová špionáž – Finanční služby	2,0 miliardy liber
Průmyslová špionáž – Těžební průmysl	1,6 miliard liber
Ztráta zákaznických dat (nejlepší scénář)	0,96 miliard liber
Online krádež na úkor subjektů byznysu (nejpravděpodobnější scénář)	1,3 miliardy liber
Vydírání (nejpravděpodobnější scénář)	2,2 miliardy liber

Zdroj: Detica (2011)

34 Antivirus.

Odhad provedený v rámci studie Detica (2011) byl založen na nástinu nákladů z roku 2010; tam, kde nebyly k dispozici vhodné údaje, byly použity nejlepší alternativní zdroje a tato data byla zpracována stejným způsobem jako ta ostatní.

Je třeba poznamenat, že odhady nákladů ze strany Detica (2011) měly řadu omezení. Mnoho z nich se souvisí s předpoklady autorů, které hrály důležitou roli v dosažení odhadů uvedených ve zprávě. Jejich příklady jsou následující:

- pouze 1 z 15 případů je oznámen občany;
- 25 % podvodů spojených s identitou je spácháno online;
- všechny nelegální útoky ohlášené National Fraud Authority (NFA) Annual Fraud Indicator byly kybernetické.

Přesnost těchto předpokladů je pravděpodobně podstatná pro hodnocení úrovně spolehlivosti, kterou lze uvedeným odhadům nákladů přiřknout. K řadě domněnek navíc nebyly uvedeny dostatečné podrobnosti, například:

- dopad na výnosy společnosti, jestliže může konkurenční společnost využít ukradené duševní vlastnictví (předpokládaný dopad na výnosy není specifikován);
- podíl přidané hodnoty hospodářského sektoru vůči ekonomice UK, která závisí ve velké míře na hospodářské soutěži (podíl není specifikován);
- pravděpodobnost, že přidaná hodnota hospodářského sektoru bude předmětem kybernetických útoků (pravděpodobnost není specifikována).

Nedostatek transparentnosti spojený s vytvářením a použitím takových domněnek dále omezuje stupeň spolehlivosti, kterou lze přisoudit uvedeným odhadům nákladů.

K problémům s transparentností domněnek a kalkulací použitých ve výzkumu se přidává i řada metodologických rozhodnutí ze strany Detica, která by mohla ovlivnit spolehlivost výsledků. Například rozhodnutí nevzít v úvahu náklady spojené s tím, že firmy bohaté na duševní vlastnictví navyšovaly svoji kybernetickou ochranu (protože autoři pokládali tyto náklady za náklady související s obvyklým podnikáním), nebo rozhodnutí vyloučit náklady vázané na jednotlivce při předvídání kybernetické kriminality (např. firewall, antivirus). Tyto úvahy posilují obavy ohledně spolehlivosti celkového odhadu nákladů ve výši 27 miliard liber, stejně jako různých nižších odhadů, které přispěly k tomuto celkovému výpočtu.

Anderson, Barton, Bohme, Clayton, van Eeten, Levi, Moore and Savage, 2012

Anderson a kol. (2012) publikovali svoji zprávu *Measuring the cost of cyber crime* v reakci na obavy týkající se předchozích zpráv, zejména zprávy Detica (2011), která podle řady odborníků náklady spojené s kybernetickou kriminalitou nadhodnotila. Zpráva se přidržuje následujících definic kybernetické kriminality navržených Evropskou komisí v roce 2007.

- Tradiční formy trestné činnosti jako podvod (fraud) nebo padělání (forgery), která je spáchána s použitím elektronických komunikačních sítí a informačních systémů.
- Publikace nelegálního obsahu pomocí elektronických médií (např. sexuální vykořisťování dětí nebo podněcování rasové nenávisti).
- Kriminalita páchaná výlučně prostřednictvím elektronických sítí, např. útoky proti informačním systémům, DoS nebo hacking.

Pro analýzu nákladů spojených s kybernetickou kriminalitou podle uvedených definic autoři odhadli celosvětové částky. Pracovali s předpokladem, že UK reprezentuje přibližně 5 % světového HDP a podle toho nastavili odhady jednotlivých států. Autoři uvádějí, že tam, kde tento přístup nebyl vhodný, je to ve zprávě uvedeno, a „*je na tuto skutečnost brán patřičný ohled*". Autoři zohlednili přístup, který byl použit ve výzkumu Detica (2011):[35]

- odhad nákladů anticipace kybernetické kriminality;
- náklady dopadu kyberkriminality;
- náklady vynaložené v reakci na kybernetickou kriminalitu; a
- nepřímé náklady jako poškození dobré pověsti.

Autoři vyjádřili obavu týkající se této metodologie, protože „náklady dopadu kyberkriminality" zahrnují jak přímé, tak i nepřímé náklady; autoři tvrdí, že nepřímé náklady je obtížnější přesně odhadnout než přímé náklady. Domnívají se navíc, že náklady vynaložené v reakci na kybernetickou kriminalitu zahrnuly pouze přímé náklady. V reakci na tyto obavy Anderson a kol. navrhli přístup, který považovali za jasnější, v němž přímé a nepřímé náklady oddělili. Zahrnuli rovněž náklady na zabezpečení, náklady pro společnost a náklady příležitosti spojené se sníženou důvěryhodností online transakcí. Zpráva ve svém výzkumném rámci používá následující definice:

- přímé ztráty: peněžní ekvivalent ztrát, škod nebo jiné újmy z hlediska oběti jako dopad kybernetické kriminality.
- nepřímé ztráty: peněžní ekvivalent ztrát a nákladů příležitosti, které jdou na újmu společnosti vůbec a vyplývají z faktu, že došlo k určitému kybernetickému trestnému činu, bez ohledu na to, zda úspěšně či nikoliv a nezávisle na konkrétním případu.
- náklady na obranu: peněžní ekvivalent preventivních opatření.

Náklady použité v analýze byly převzaty z různých výzkumných a statistických zdrojů nalezených v literatuře a tam kde to bylo nezbytné, se autoři dobrali různých odhadů nákladů pro UK pomocí domněnek. Výběr ze shrnující tabulky je zde uveden jako příklad (Tab. A1.4).

Tabulka A1.4: Odhady nákladů spojených s kybernetickou kriminalitou podle Andersona a kol. (2012)

Typ kybernetické kriminality	Odhad pro UK	Celosvětový odhad	Období
Náklady ryzí kybernetické kriminality			
Online bankovní podvody			
- **Phishing**	16 milionů $	320 milionů $	2007
- **Malware (zákazník)**	4 miliony $	70 milionů $	2010
- **Malware (byznys)**	6 milionů $	1 milion $	
- **Technická opatření bank**	50 milionů $	1 miliarda $	2010
Falešný antivirus	5 milionů $	**97 milionů $**	2008-2010
Software porušující autorská práva	1 milion $	**22 milionů $**	2010

35 A ve zprávě Economic and Social Costs of Crime (Home Office, 2000).

Typ kybernetické kriminality	Odhad pro UK	Celosvětový odhad	Období
Hudba aj. obsah porušující autorská práva	7 milionů $	**150 milionů $**	2011
Farmaceutika porušující patentová práva	14 milionů $	**288 milionů $**	2010
Podvod: přítel v nesnázích	1 milion $	**10 milionů $**	2011
Falešná úschova[36]	10 milionů $	**200 milionů $**	2011
Zálohový podvod[37]	50 milionů $	1 miliarda $	2011
Náklady platebních podvodů			
Podvod při online platbě kartou	210 milionů $	4,2 miliardy $	2010
Podvod při offline platbě kartou			
- **Vnitrostátní**	106 milionů $	2,1 miliardy $	2010
- **Mezinárodní**	147 milionů $	2,94 miliardy $	2010
- **Náklady na obranu bank/ obchodníků**	120 milionů $	2,4 miliardy $	2010
Nepřímé náklady platebních podvodů			
- **Ztráta důvěry (zákazníci)**	700 milionů $	10 miliard $	2010
- **Ztráta důvěry (obchodníci)**	1,6 miliardy $	20 miliard $	2009
PBX podvod[38]	185 milionů $	**4,96 miliard $**	2011

Pozn. Tučně vytištěná čísla jsou odhady založené na datech nebo domněnkách v dané oblasti. Nezvýrazněná čísla byla stanovena pomocí podílu UK na světovém hrubém domácím produktu, není-li uvedeno jinak.

Zdroj: Anderson a kol. (2012)

V této shrnující tabulce byly zaznamenány pouze ty trestné činy, jejichž celosvětové náklady přesáhly 10 milionů USD. Čísla, která nebyla vytištěna tučně, byla získána přepočtem vycházejícím z podílu UK na celosvětovém HDP.

Je obtížné odhadnout spolehlivost řady hodnot uvedených v Tabulce A1. 4. Zčásti je to z důvodů závislosti na práci ostatních, kteří zjišťují dílčí hodnoty, na nichž je postavena analýza. Mimoto Anderson a kol. (2012) vytvořili řadu domněnek, jejichž odůvodnění není zcela zřejmé. Viz například následující výňatek ve vztahu k odhadu nákladů na záplatování.

„Část těchto nákladů, kterou lze přičíst UK, bude pravděpodobně odpovídat nanejvýš podílu UK na globálním HDP, protože softwarový průmysl UK je v porovnání s USA proporcionálně menší. Pro ilustraci předpokládejme, že celkové náklady spojené se záplatováním

36 Podvodný vázaný svěřenecký účet – pozn. překl.

37 Podvod spojený se zaplacením zálohy a dalších poplatků – pozn. překl.

38 Neoprávněné napojení se na telefonní systém (PBX) napadené společnosti, označované i jako phreaking – pozn. překl.

představují 1 miliardu USD ročně, na UK v takovém případě připadne 50 milionů USD z této celkové částky. Tyto náklady nezahrnují náklady na aplikaci záplat, které nesou koncoví uživatelé" (Anderson a kol., 2012, str. 22).

Zmíněný výňatek žádným způsobem nenaznačuje, odkud se vzal náklad globální ekonomiky ve výši 1 miliardy USD, a je též proto obtížné odhadnout spolehlivost odhadu nákladů ve výši 50 milionů USD.

Dále jsou zde omezení vyplývající ze závislosti použitého přístupu na HDP, protože „*výpočet odhadů pro UK vycházející z podílu na celkových nákladech kriminality ve vztahu k HDP závisí jak na přesnosti použitých celosvětových odhadů, tak na předpokladu, že relativní část trestných útoků v UK vždy odpovídá jejich nákladům v poměru k HDP*", (Home Office, 2013c).

Měli bychom zmínit, že zpráva Andersona a kol. nezahrnuje čísla pro průmyslovou kybernetickou špionáž a vydírání, poněvadž „*není žádný spolehlivý důkaz o rozsahu nebo nákladech spojených s průmyslovou kybernetickou špionáží a vydíráním*". Předpokládáme-li však, že tento odhad zahrnuje velkou část (2,2 miliardy liber) celkového odhadu nákladů spojených s kybernetickou kriminalitou uvedeného ve zprávě Detica (2011), pak nezahrnutí kybernetické špionáže a vydírání do odhadů ve zprávě Andersona a kol. částečně vysvětluje značné rozdíly v celkových odhadech. Ačkoli Anderson a kol. konstatují, že odhady učiněné Deticou neměly „*jednoznačné základy*", řada zpráv týkajících se jiných států pronikajících do počítačových sítí vlád a korporací, pravděpodobně s cílem získat utajované informace aj., svědčí o tom, že jakýkoli odhad, který nezahrnuje náklady spojené s krádeží duševního vlastnictví a obchodně citlivých informací, může náklady spojené s kybernetickou kriminalitou silně podhodnocovat.

Oxford Economics, 2014

Studie Oxford Economics o vlivu kybernetických útoků na společnosti v UK byla publikována na žádost Centre for the Protection of National Infrastructure (CPNI) a měla zkoumat vliv státem sponzorovaných kybernetických útoků na firmy v UK. Kromě vytvoření ekonomického rámce pro porozumění těmto dopadům studie též zahrnula:

- výzkum mezi firmami v UK s cílem odhadnout náklady dopadů kybernetických útoků;
- případovou studii zkoumající dopady kybernetických útoků na tržní prostředí; a
- řadu případových studií dokládajících zkušenosti britských firem s kybernetickými útoky.

Ve zprávě autoři stručně hovoří o typologii z hlediska nákladů spojených s kybernetickou kriminalitou a přijímají model Home Office (2000):

- náklady anticipace;
- náklady dopadu; a
- náklady vynaložené v reakci.

Výsledky výzkumu prezentované ve zprávě jsou založeny na online dotazníku distribuovaném e-mailem na adresy uvedené v databázi IT odborníků, IT pracovníků zaměřených na bezpečnost a dalších IT specialistů. Tato databáze byla vybrána jako vhodný vzorek,

neboť byla již dříve využívána při podobných výzkumech prováděných ze strany Ponemon Institute – subdodavatel zodpovědný za provedení průzkumu. Z celkem 9 973 rozeslaných dotazníků jich bylo zodpovězených 427, přičemž návratnost 4,3 % byla autory hodnocena jako pro tento obor nadprůměrná. S ohledem na způsob výběru nemohou být výsledky tohoto výzkumu považovány za reprezentativní z hlediska firem v UK jako takových.

Výsledky výzkumu ukázaly, že 60 % respondentů bylo v uplynulých 12 měsících vystaveno kybernetickému útoku a z nichž 31 % uvedlo, že v souvislosti s útokem došlo ke ztrátě citlivé informace. U těchto ani jiných výzkumných otázek autoři neposkytli informaci o tom, kolik respondentů na tuto otázku neodpovědělo. Je také třeba poznamenat, že kladná odpověď na tuto otázku předpokládá, že si je podnikatelský subjekt vědom toho, že byl vystaven kybernetickému útoku a osoba odpovídající v rámci dotazníku byla o tomto útoku rovněž informována – vzhledem k tomu může být skutečný podíl podnikatelských subjektů, které se staly cílem kybernetického útoku v uplynulých 12 měsících, vyšší než referovaných 60 %.

Ve výzkumu bylo rovněž uvedeno několik odhadů ztrát jako důsledku kybernetických útoků.

Tabulka A1.5: Náklady britských firem v souvislosti s kybernetickými útoky za 24 měsíců (v milionech liber).

Položka	Clean-up / vyléčení (n=375)	Ztracená produktivita (n=375)	Narušené operace (n=375)	Poškození / krádež IT (n=371)	Dobré jméno / značka (n=272)
Průměr	2,3	1,9	2,3	1,9	2,9
Adjustovaný průměr	0,8	0,9	0,8	0,8	0,9
Medián	0,18	0,18	0,18	0,18	0,38

Zdroj: Oxford Economics (2014)

Autoři poznamenávají, že kritici předchozích studií zpochybnili užitečnost průměrů uváděných v těchto výzkumech z hlediska spolehlivosti vzhledem k velkému množství odlehlých hodnot a malé velikosti vzorků. Autoři reagují na tuto kritiku důrazem na účel jejich výzkumu, ve kterém nejde o extrapolaci na všechny podnikatelské subjekty v UK, ale spíše o vyzdvižení výsledků sledovaného vzorku (Oxford Economics, 2014, str. 3). Ve výše uvedené tabulce adjustovali průměry tak, že vyloučili odlehlé hodnoty – pozorování lišící se od průměru o více než 2,5 – a uvedli současně hodnotu mediánu.

Výzkum rovněž zahrnul coby důsledek kyberútoků ztrátu duševního vlastnictví a obchodně citlivých informací (Tabulka A1.6).

Tabulka A1.6: Náklady britských firem v souvislosti se ztrátou duševního vlastnictví a obchodně citlivých informací jako důsledek kybernetických útoků v průběhu předchozích 24 měsíců.

Položka	Náklady: DV (n=69)	Náklady: obchodně citlivé informace (n=69)
Průměr	17,3	15,1
Adjustovaný průměr	13,2	12,8
Medián	7,5	7,5

Zdroj: Oxford Economics (2014)

Autoři též poznamenávají, že je důležité vzít v úvahu, že 80 % respondentů uvedlo, že v předchozích 24 měsících neutrpěli žádnou ztrátu duševního vlastnictví ani obchodně důležitých informací. Podle autorů sice prezentované výsledky výzkumu nelze zobecňovat, ale možná naznačují, že ačkoliv utrpí tyto ztráty pouze menšina podnikatelských subjektů, jejich náklady jsou vyšší než jiné náklady vyvstávající coby důsledek kybernetického útoku.

Kromě výše uvedených výsledků též zpráva podrobně vylíčila případovou studii, která analyzovala potenciální ztráty v souvislosti s poškozením dobré pověsti, spolu s několika příklady firem vystaveným kybernetickému útoku a zvážením, jak tyto útoky ovlivnily jejich činnost. Poškození dobré pověsti bylo vyjádřeno jako snížení hodnoty na akciovém trhu, ke kterému může dojít bezprostředně po zveřejnění zprávy o proběhnuvším kybernetickému útoku. Prozkoumáním průměrných abnormálních výnosů autoři zjistili, že ve více než polovině případů útoků byly negativní, což poukázalo na záporné ovlivnění na burze cenných papírů jako důsledek kybernetického útoku. Statisticky významné výsledky však byly nalezeny pouze u tří takových firem. U nich se lze domnívat, že utrpěly ztrátu dobré pověsti vedle dalších nákladů spojených s kybernetickými útoky, kterým byly vystaveny.

Ponemon Institute, 2015

Každoroční studie Ponemon Institute (2015) týkající se nákladů britských firem spojených s kybernetickou kriminalitou zkoumala celkové náklady, které tyto organizace musely vynaložit v souvislosti s kybernetickými útoky, včetně:

- detekce, vyšetřování a vyhrocení;
- zamezení šíření;
- obnovy;
- následné reakce;
- snahy snížit vliv útoku z hlediska ztráty nebo zcizení informací, narušení obchodní činnosti a poškození vybavení; a
- ztráty příjmů.

Autoři definují kybernetický útok jako: „*Trestnou činnost realizovanou pomocí internetu. Tyto útoky mohou zahrnout krádež duševního vlastnictví, zabrání online bankovních účtů, vytvoření a rozšíření virů na jiné počítače, zveřejnění důvěrných obchodních informací na Internetu nebo narušení národní kritické infrastruktury daného státu*" (Ponemon Institute, 2015, str. 1).

Metodologie použitá Ponemon Institute zahrnula 326 rozhovorů se zaměstnanci 39 velkých organizací. Jak autoři ve zprávě konstatují, „*každá roční studie zahrnuje různý vzorek subjektů. Jinými slovy, nesledujeme stejný vzorek subjektů v čase*" (str. 2). Proto rozdíly mezi odhady z roku na rok mohou reflektovat spíše rozdíly mezi subjekty než skutečné změny nákladů.

Ponemon Institute v roce 2015 zjistil, že průměrné roční náklady pro 39 korporací činily 4,1 milionu liber za rok (medián 3,4 milionu liber), což reprezentovalo 14 % přírůstek oproti roku 2014, v rozmezí mezi 628 423 a 16 miliony liber. Tyto náklady byly odhadnuty prostřednictvím požadavků na zaměstnance, aby hlásili náklady spojené s kybernetickými útoky v období čtyř týdnů, přičemž tyto pak byly použity pro odhad celoročních nákladů. Ze zprávy není jasné, zda se jednalo o poslední uplynulé nebo typické čtyřtýdenní období. Náklady se nicméně významně lišily v závislosti na zkoumaném průmyslovém segmentu. Například v roce 2015 se společnosti působící v oblasti financí, energetiky a technické infrastruktury a společností v oblasti komunikací potýkaly s vyššími náklady spojenými s kyberkriminalitou než maloobchodní společnosti, veřejný sektor, vzdělání a výzkum. Uvedený výzkum dále zjistil, že velikost organizace pozitivně korelovala s ročními náklady spojenými s kybernetickou kriminalitou. Zpráva Ponemon Institute (2015) rovněž odhadla, že narušení obchodní činnosti a ztráta příjmů představovaly dva nejvyšší externí náklady, zatímco obnova a detekce byly nejnákladnějšími interními činnostmi.

Ponemon Institute (2015) uvádí některá omezení vyplývající z použitých metod. Ty snižují možnost generalizace výsledků a při uvažování nad zjištěnými odhady by měly být vzaty v potaz. Některá z omezení týkající se tohoto výzkumu spočívají v tom, že Ponemon Institute (2015), podobně jako jiné společnosti, používal svůj vlastní benchmark, který nedovoluje vnější přezkoumání. Metodologie navíc zahrnuje:

- vzorek, který nedovoluje činit statistické závěry;
- zkreslení v důsledku non respondence;
- způsob výběru vzorku, o němž Ponemon Institute předpokládal, že zahrnuje společnosti s vyspělejšími informačními bezpečnostními programy; a
- polehání se na čestnost respondentů.

Centre for Economics and Business Research, 2015

Zpráva Centre for Economics and Business Research (Cebr) za rok 2015 poskytuje informace o tom, jak vnímá kybernetickou bezpečnost a náklady spojené s kybernetickými útoky tzv. C-level (hovorový výraz pro vrcholný management obvykle nazývaný ředitelé). Zpráva uvádí, že: „*výzkum a data shromážděná v rámci Annual Business Survey (ABS) umožnila Cebr odhadnout počet podnikatelských subjektů postižených kybernetickou kriminalitou. Cebr rovněž odhadl ztrátu příjmů v důsledku kybernetické kriminality v UK a míru růstu IT nákladů v reakci na prolomení kybernetické bezpečnosti*".

Cebr zjistil, že 15 % firem v UK oznámilo prolomení zabezpečení, které vedlo ke ztrátě příjmů. Největší obavy respondentů týkající se kybernetických útoků byly náklady spojené s prolomením zabezpečení, včetně (ale nejen) nákladů na:

- forenzní zkoumání;
- clean-up;

- právní výlohy;
- poškození dobré pověsti a obchodní značky spojené se ztrátou zákaznických dat; a
- ztrátu příjmů v důsledku odstávky.

Cebr odhadl, že kybernetické útoky způsobily ztráty příjmů firem v UK ve výši 18 miliard liber. Firmy navíc utratily téměř 16 milionů liber v následných platbách IT sektoru v reakci na narušení kybernetické bezpečnosti. Téměř všechny firmy (88 %) oznámily, že zvýšily své roční IT náklady, aby čelily budoucím útokům. Většina vedoucích technologických oddělení (70 %) se domnívá, že jejich stávající strategie kybernetické bezpečnosti blokuje inovace, což naznačuje nepřímé náklady spojené se zvyšováním bezpečnosti. Zpráva rovněž zjistila, že ačkoliv byla u britských podnikatelských subjektů spojena jedna třetina kybernetické kriminality s krádeží duševního vlastnictví, respondenty byla hodnocena jako šestá nejvyšší priorita.

Ze studie není jasné, jak byl zkoumaný vzorek vybírán, jak reprezentativní byl z hlediska širší populace nebo kolik oslovených ve výzkumu opravdu odpovědělo. Proto není jasné, do jaké míry lze výsledky studie generalizovat.

Příklady zpráv souvisejících s odhady podvodů

Financial Fraud Action UK, 2015

Financial Fraud Action UK (FFA UK) *„je zodpovědná za vedení kolektivního boje proti podvodům v sektoru zabývajícím se platbami v UK"* a její *„instituce zahrnují banky, vydavatele kreditních, debetních a nákupních karet a příjemce plateb v UK"* (Financial Fraud Action UK, 2015, str. 2). Ve své zprávě FFA UK odhaduje, že ztráty vyplývající z podvodů, jež se týkaly karet vydaných v UK, dosáhly v roce 2014 celkové sumy 479 milionů liber, což představovalo 6 % nárůst proti předchozímu roku. Z toho 217,4 miliony liber představovaly podvody spojené s internetovým obchodem a 60,4 milionů liber podvody v oblasti internetového bankovnictví. FFA UK též poskytla odhady týkající se jiných kategorií podvodů mimo online prostředí, hovoří o tom, jak jsou podvody obecně páchány a dává zákazníkům tipy z hlediska bezpečnosti. Zpráva však neuvádí žádné podrobnosti, jak byly odhady a náklady shromážděny a uspořádány.

Zpráva nabízí také souhrn všech opatření přijatých karetním průmyslem během posledních 10 let, které prokazatelně snížily ztráty spojené s podvody. Nebyl v ní však uveden odhad částky vynaložené v souvislosti s těmito činnostmi. Mezi opatřeními zmiňovanými ve zprávě jsou:

- Dedicated Card and Payment Crime Unit (DCPCU), údajně od svého vzniku zabránila ztrátám ve výši 470 milionů liber;
- Financial Fraud Bureau (FFB);
- Fraud Intelligence Sharing System (FISS);
- American Express Safekey,
- MasterCard SecureCard;
- Verified by Visa;
- Address Verification Services (AVS) a Card Security Code (CSC);
- Cyber Streetwise;

- Chip and Pin, inteligentní systémy detekce podvodů využívané bankami;
- průmyslová opatření zabraňující zneužívání bankomatů;
- průmyslová opatření chránící zákazníky před šekovými podvody; a
- průmyslová opatření na ochranu před podvody s elektronickým a telefonním bankovnictvím.

Odhady nákladů těchto opatření by poskytly další poznatky k nákladům spojeným s anticipací a prevencí různých forem podvodů.

Data publikovaná FFA UK patří v současné době pravděpodobně k těm nejspolehlivějším, která jsou k dispozici a na jejichž základě můžeme začít odhadovat celkové náklady spojené s kybernetickou kriminalitou v UK. Je to umožněno porovnáváním informací přímo poskytovaných bankami, subjekty vydávajícími kreditní karty, debetní karty a úvěrové karty, jakož i příjemci karetních plateb v UK, přičemž se tyto informace týkají všech aktuálních případů podvodů a s nimi spojených ztrát. Data jsou shromažďována v souladu s definicemi a kategoriemi používanými v průmyslu a kromě toho, že FFA UK umožňuje provádět odhady, rovněž přispívá k diskusím o tom, jakým způsobem jsou podvody páchány, a dává spotřebitelům tipy, jak dosahovat vyšší bezpečnosti.

Zpráva FFA UK však neobsahuje podrobnosti o tom, jak byly publikovaná čísla a náklady shromážděny a uspořádány. Dále zpráva uvádí řadu opatření, která subjekty zajišťující platební styk pomocí karet v minulých deseti letech přijaly, a která údajně snížila ztráty působené podvody. Například Dedicated Card and Payment Crime Unit (DCPCU) uvádí, že od svého založení zabránila ztrátám ve výši 470 milionů liber. Chybí však odhady nákladů této činnosti. Ty by poskytly bližší poznatky o nákladech vynaložených na anticipaci nebo jako prevence různých forem podvodů.

British Retail Consortium, 2015

BRC (2015) uvedlo, že celkové náklady spojené s trestnou činností v maloobchodním sektoru UK v období 2013-2014 činily 603 miliony liber, což představovalo nárůst o 18 % oproti předchozímu roku; 223 miliony liber z této částky představují ztráty způsobené podvody. Odhaduje, že online bylo spácháno 69 % podvodů s kreditními/debetními kartami, 33 % podvodů s úvěrovými účty, 10 % podvodů při refundaci a 10 % podvodů s vouchery a dárkovými kartami. Ve zprávě se rovněž uvádí, že většina respondentů prohlašovala, že počty případů kybernetické kriminality byly buď stejné nebo vyšší ve srovnání s předchozím rokem.

Většina respondentů uvádí jako kritické následující hrozby:
- krádež dat (77 %);
- hacking (68 %);
- odmítnutí služby (DoS) (64 %);
- extrakce dat z internetu (scraping) (64 %); a
- škodlivý software (55 %).

Zpráva BRC neuvádí podrobnosti o vytvoření sledovaného vzorku, ale prohlašuje, že „*pokryl 50 % obratu maloobchodního sektoru a týkal se 1,6 milionu zaměstnanců*", (str. 10).

Vzhledem k nedostatku dostupných podrobnějších údajů, které by popisovaly použité metody, není zřejmé, jak jsou výsledky výzkumu spolehlivé, jak jsou reprezentativní z hlediska maloobchodního sektoru jako celku a zda jsou učiněné extrapolace platné.

National Fraud Authority, 2013

National Fraud Authority (2013) také usilovala o odhady ztrát způsobených podvody v řadě sektorů. Pracovala se zainteresovanými osobami v různých sektorech a učinila celkové odhady na základě primárních dat získaných výzkumem a sekundárních dat od svých partnerů. Zpráva NFA (2013) uvádí, že její odhady nutně nemusí být meziročně srovnatelné vzhledem k vylepšování metodologie; její odhady by však měly být považovány za „*nejlepší odhad možné velikosti problému*", (str. 4). Je též třeba zmínit, že tyto odhady používají:

- sekundární data, z nichž ne všechna jsou spolehlivá;
- výzkumy využívající nenáhodný výběr vzorku, které proto pravděpodobně nejsou reprezentativní; a
- data uvádějící střední průměrné ztráty, která jsou pravděpodobně zkreslena anomáliemi.

Zpráva z roku 2013 odhaduje náklady spojené s podvody v rámci ekonomiky UK na 52 miliard liber. Toto číslo, jako mnoho jiných ve zprávě, není rozděleno na podvody prováděné online a offline. NFA např. odhaduje, že přímé a skryté náklady způsobené podvody činily ročně 6,7 miliardy liber pro velké a 9,2 miliardy liber pro malé či střední podniky. Veřejný sektor měl vydat na přímé a skryté náklady spojené s podvody 20,6 miliardy liber. Tato hodnota zahrnuje zejména příjmy z daní, dávky a dotace, ale nikoliv náklady na prosazení práva. Dobročinné organizace měly být podvodně připraveny o 147,3 milionu liber pomocí online i offline podvodů, včetně podvodů při platbách, podvodů učiněných zaměstnanci a dobrovolníky, jakož i kybernetických podvodů.

Další odhady poskytují o něco lepší vhled do podílu podvodů usnadněných díky ICT. Např. roční ztráty finančního sektoru skrze podvody měly činit 5,4 miliardy liber, z čehož 40 milionů liber byly podvody spojené s online bankovnictvím a 388 milionů liber podvody spojené s užíváním karet. Ztráty způsobené podvody jednotlivcům činily 9,1 miliardy za rok. National Fraud Authority rozdělila tento odhad na následující položky:

- hromadné marketingové podvody - 3,5 miliardy liber (velká část z této částky byla pravděpodobně způsobena kybernetickými podvody);
- podvody spojené s identitou - 3,3 miliardy liber (značnou část rovněž mohly tvořit kybernetické podvody);
- podvody s online prodejem lístků - 1,5 miliardy liber (všechny podvody kybernetické);
- podvody týkající se nájemného - 755 milionů liber; a
- podvody s předplacenými měřiči elektřiny - 2,7 milionu liber.

Sektor poskytovatelů zabezpečení (security providers)

V posledních letech se stalo běžné, že poskytovatelé zabezpečení vytvářejí odhady týkající se nákladů spojených s kybernetickou kriminalitou, které posilují potřebu jejich produktů. Čtenáři si musí být vědomi, že všechny tyto zprávy publikované výrobci/dodavateli softwaru mají zvýšit poptávku/hodnotu jimi nabízených produktů. Tak jako tomu je v případě všech zpráv publikovaných výrobci a dodavateli softwaru, musí si být jejich

čtenáři vědomi, že tyto zprávy jsou vydávány, aby podporovaly u uživatelů potřebu používání těchto produktů a propagovaly jejich kvalitu. Širší paleta omezení navázaných na měření uváděná v těchto bezpečnostních zprávách je zmíněna také v Home Office (2013c).

Zpráva McAfee/Intel (2014) se pokusila odhadnout celosvětové náklady spojené s kybernetickou kriminalitou. Autoři poznamenávají, že jejich odhad „*se zaměřuje na přímé i nepřímé náklady a na data, která berou v úvahu ztrátu duševního vlastnictví, odcizení majetku a citlivých obchodních informací, náklady (obětované) příležitosti, dodatečné náklady na zabezpečení sítě a náklady na odstranění následků kybernetických útoků včetně poškození dobré pověsti subjektu vystaveného hackerskému útoku*", (str. 4).

I McAfee/Intel shledává problematickými náklady, které se týkají odcizeného duševního vlastnictví. Autoři píší: „*odhadování nákladů spojených s krádežemi duševního vlastnictví je mezi náklady spojenými s kybernetickou kriminalitou nejnáročnější, ale současně se jedná o nejdůležitější proměnnou při určování výše ztrát",* (str. 6).

Na základě tohoto rámce autoři uvádějí, že celosvětové náklady spojené s kybernetickou kriminalitou mohou být:

- 375 miliard USD (konzervativní odhad získaný extrapolací dat z otevřených zdrojů);
- 445 miliard USD (odhad získaný souhrnem nákladů coby podílů regionálních příjmů); nebo
- až 575 miliard USD (extrapolace dat ze ztrát zemí s vysokými příjmy).

Autoři dále udávají (s nízkým intervalem spolehlivosti), že podíl HDP, který je ztracen v důsledku kybernetické kriminality v UK, je 0,16 %. Neposkytují však důkazy pro tento odhad. Zpráva také spíše čerpá z předchozích výzkumů, např. Anderson a kol. (2012), než z nového primárního výzkumu.

Naproti tomu Symantec (2013) uvádí mnohem nižší odhady. Symantec provedl online výzkum zahrnující více než 13 000 respondentů ve věku 18-64 let, který pokryl 24 zemí. Měli bychom zmínit, že obvyklá omezení týkající se vzorku v online výzkumu platí i zde. Nemůžeme si být jisti, zda je takto prováděný výzkum reprezentativní pro širší populaci. V rámci UK představoval vzorek 500 dospělých respondentů. Symantec uvádí, že celosvětové (na základě zkoumaných 24 zemí) celkové náklady spojené s kybernetickou kriminalitou v uplynulých 12 měsících činily 113 miliard USD, přičemž průměrné přímé náklady vypočítané na subjekt postižený kybernetickou kriminalitou činily 298 USD. Pro UK autoři odhadují, že celkové náklady spojené s kybernetickou kriminalitou za uplynulých 12 měsíců činily 1 miliardu USD s průměrnými přímými náklady vypočítanými na subjekt postižený kybernetickou kriminalitou ve výši 101 USD. Zpráva odhaduje 12 milionů obětí kyberkriminality v uplynulých 12 měsících předcházejících výzkumu. McAfee/Intel se domnívají, že náklady kyberkriminality jsou podhodnocené vzhledem k nehmotným hodnotám a „skutečným" nákladům globální ekonomiky a národní bezpečnosti.

Verizon (2015) referoval o předpokládaných finančních nákladech pro společnosti, u nichž došlo k prolomení ochrany dat, a to na základě množství odcizených záznamů. Tato zpráva za rok 2014 zahrnula 70 organizací v 61 zemích a uvádí, že došlo k:

- 79 790 bezpečnostním incidentům (definovaným jako jakákoli událost, která narušila důvěrnost, integritu nebo dostupnost informační položky); a
- 2 122 potvrzeným případům úniku dat (definovaných jako incident, jehož výsledkem bylo potvrzené prozrazení neautorizovanému subjektu, nikoli jenom ohrožení).

Ačkoli Verizon zjistil, že žádné průmyslové odvětví není vůči prolamování ochrany dat imunní, nejvíce zkušeností s potvrzeným prolomením zabezpečení vedoucím ke ztrátě dat měly státní, informační a finanční služby. Zpráva dále predikovala náklady prolomení ochrany dat na základě rozsahu prolomení, měřeno počtem ukradených záznamů (100; 1 000; 10 000; 100 000; 1 000 000; 10 000 000; 100 000 000). Například suma 1 258 670 USD představuje očekávané finanční náklady společnosti v souvislosti s odcizením 1 milionu záznamů (průměr byl mezi 892 400 a 1 775 350 USD a odhad mezi 57 600 a 27 500 090 USD).

Neustar (2015) zjistil, že polovina podnikatelských subjektů oznámila, že útoky mající za následek odmítnutí služby (DoS) nebo distribuované odmítnutí služby (DDoS) se staly větší hrozbou než v předcházejícím roce. Bylo zajímavé, že většina společností, které považovaly DDoS útoky za menší hrozbu, přesto investovala do ochrany proti nim více. Více než čtvrtina společností uvedla, že DDoS útoky ohrožují především obchodní značku/důvěru zákazníků. Každá třetí z napadených společností uvedla, že útok trval 1-2 dny. Polovina napadených společností se rovněž stala obětí krádeže zákaznických dat, duševního vlastnictví nebo finančních prostředků. Ve svém vzorku 250 odborníků Neustar (2015) zjistil, že 22 % společností ohlásilo ztráty příjmů ve výši mezi 50 000 a 99 999 liber za hodinu v důsledku výpadku provozu ve špičce (šlo o nejčastější odpověď). Dále:
- 16 % oznámilo, že jejich ztráty přepočtené na hodinu byly nižší než 30 000 liber;
- 12 % oznámilo ztráty mezi 30 000 a 49 999 liber;
- 16 % mezi 100 000 a 299 999 librami;
- 11 % mezi 300 000 a 600 000 librami;
- 12 % více než 600 000 liber; a
- 11 % neznalo náklady výpadku provozu.

Policie londýnské City (2015)

Ve své zprávě z roku 2015 o dopadu ekonomické kybernetické kriminality na činnost policie se autoři zaměřili na tři hlavní formy ekonomické kybernetické kriminality:
- kriminalita závislá na ICT;
- kriminalita usnadněná ICT; a
- kriminalita uskutečněná s pomocí ICT.

Při zkoumání těchto forem kybernetické kriminality autoři provedli původní výzkum na výběru dat FFA UK, z nichž vyvodili a publikovali řadu poznatků. Tato zjištění zahrnují odhady mediánových částek, které oběti trestné činnosti vyplatily pachatelům podvodů ve čtvrtém čtvrtletí roku 2014 – například:
- 38 974 liber za důchodové podvody;
- 28 609 liber za podvody při obchodování mezi podnikatelskými subjekty;
- 21 534 liber za podvody s finančními investicemi; a
- 20 000 liber za konkurzní a insolvenční podvody.

Zpráva rovněž poskytuje odhady (střední) průměrné částky, kterou se podařilo získat zpět od podvodníků během čtvrtého čtvrtletí, například:

- 39 958 liber za podvody s finančními investicemi;
- 47 542 liber za podvody v oblasti bankovního a úvěrového sektoru;
- 35 863 liber za firemní podvody; a
- 30 904 za důchodové podvody.

Na primární analýze vybraných dat je založena i řada dalších odhadů, které mohou pomoci výzkumníkům porozumět povaze podvodů oznámených ve výzkumném vzorku.

Ačkoliv výzkum prezentovaný v této zprávě poskytuje užitečný kontext co do typu a rozsahu podvodů, o nichž hovoříme, je zde řada technických a metodologických otázek ovlivňujících hladinu spolehlivosti, kterou lze uvedeným odhadům přisoudit.

Například není vždy jasné, zda byla analýza založena na trestných činech nebo incidentech (zahrnutí incidentů by mohlo negativně ovlivnit spolehlivost kteréhokoli z následných výsledků). Analýza rovněž definuje „kybernetický prvek" na základě prvního kontaktu, což nemusí být spolehlivá indikace. Abychom uvedli příklad: použijeme-li tuto definici, pak hacking serverů zahrnuje jen 31 % podílu kybernetické kriminality, zatímco ze své povahy by tento trestný čin měl být hodnocen se 100 % podílem. Navíc vyčlenění skupiny „trestných činů uskutečněných s pomocí ICT" znamená, že výsledky této studie nejsou snadno srovnatelné s jinými studiemi, které používají definice konzistentnější s většinou literatury (např. trestné činy usnadněné ICT a závislé na ICT).

Také k údajům o nákladech uváděným samotnými oběťmi v rámci self-reportů je třeba přistupovat obezřetně, neboť mohou být zavádějící a mohou odrážet ztráty viditelné pouze v okamžiku, kdy jsou oznámeny; neberou v úvahu následné kompenzační platby. Omezením je rovněž objem chybějících dat v údajích Action Fraud.

Celkově lze konstatovat, že zmíněné skutečnosti ovlivňují spolehlivost oznámených odhadů, ale zároveň představují dobrý výchozí bod pro další výzkum.

Výnosy pachatelů

Ačkoli Pracovní skupina cítí, že je důležité se podívat na náklady z různé perspektivy, dosud nedošlo k zásadnímu pokusu zaměřit se na zkoumání zisků pachatelů spojených s kybernetickou kriminalitou. V průběhu tohoto pracovního programu Pracovní skupina zvažovala zahrnutí nákladů pachatelů a jejich zisky do výzkumného rámce kybernetické kriminality, neshledala to však vhodným. Ve světle problémů naznačených touto zprávou je jejím primárním zaměřením zkoumání nákladů vzešlých korporacím a jednotlivcům.

V této kapitole neuvádíme vyčerpávající souhrn zpráv zkoumajících zisky pachatelů, protože nejsou přímo svázány s náklady kyberkriminality. Jinými slovy náklady spojené s kriminalitou nejsou stejné jako zisky pachatelů. Ve většině případů budou přímé náklady dopadu kyberkriminality mnohem vyšší než zisky pachatelů, a to i bez zahrnutí nákladů

anticipace útoku a vynaložených v reakci na něj. V této části jsou vzata v úvahu zjištění Andersona a kol. (2012), Symantec (2015), a Ponemon Institute (2016). Většina těchto odhadů by měla být hodnocena s nejvyšší opatrností, neboť jsou:

- založeny na pohledech expertů spíše než na výzkumech kybernetické kriminality;
- extrapolovány z malých vzorků, nebo
- extrapolovány z globálních hodnot.

Zpráva Andersona a kol. (2012) uvádí výše výnosů pro širokou škálu trestných činů usnadněných a závislých na ICT. Autoři odhadují, že měsíční zisk z prodeje padělaných léčiv v roce 2010 byl 8 milionů USD a celosvětově 288 milionů USD za rok. S použitím „*pravidla 5 % podílu UK na celosvětovém HDP*" odhadli, že spotřebitelé v UK „*zaplatili zhruba 400 000 USD v rámci hlavních programů prodeje padělaných léčiv v roce 2010 a pravděpodobně celkově až 1,2 milionu měsíčně*" (str. 13) neboli 14 milionů USD za rok. Co se týká padělaného softwaru, odhaduje se, že pět hlavních organizací produkujících padělaný výukový software vykázalo v celosvětovém měřítku v roce 2011 zisk 22 milionů USD s tím, že pro UK tato částka činila 1 milion USD. Celosvětové příjmy spojené s hudbou a videem porušujícím autorská práva byly odhadnuty na 150 milionů USD (7 milionů USD v UK) a vycházely z hodnoty zabaveného majetku gangu Megaupload v Aucklandu a vynásobením jeho podílu na trhu. Celosvětové příjmy z falešného antivirového softwaru jsou odhadovány na 97 milionů USD se zhruba 5 % podílem UK.

Anderson a kol. zkoumali také zisky z různých typů podvodů, včetně přítele v nesnázích, falešné úschovy a zálohového podvodu. Na základě nepublikovaných dat zahrnujících primárně oběti z USA odhadli, že zisky v případě přítele v nesnázích v UK „*největší pravděpodobností převýšily částku 1 milion USD ročně*" (str. 15). Odhadované ztráty v UK spojené s falešnými úschovami a obvykle zhruba 100 aktivních falešných svěřeneckých webových stránek jsou vyčísleny na 10 milionů USD za rok. Na závěr autoři uvedli, že zálohový podvod „*se zdá být lukrativnější než podvody typu přítel v nesnázích nebo falešné úschovy*" (str. 16). Odhadli tyto ztráty na 50 milionů USD, avšak dodávají, že „*budeme první, kdo připustí, že toto číslo je pouze orientační a nemáme žádný skutečný důkaz, který je podporuje*" (str. 16).

Zpráva Symantec (2015) uvádí hodnotu určitých produktů v ilegální ekonomice. Píše se v ní, že „*celkově značně poklesly ceny za e-maily, poněkud poklesly za informace o kreditních kartách a za podrobnosti o online bankovních účtech zůstávají stejné*" (str. 88). Dochází též k závěru, že „*ceny v ilegální ekonomice jsou stabilní, což naznačuje stále vysokou poptávku po ukradených identitách, malwaru a službách elektronického zločinu*" (str. 88). Symantec uvádí ceny za různé typy informací prodávaných v roce 2014 na černém trhu:

- 1 000 ukradených e-mailových adres za 0,50 až 10 USD;
- podrobnosti o kreditních kartách v rozsahu 0,50 až 20 USD;
- naskenované nebo skutečné cestovní pasy měly hodnotu 1 až 2 USD;
- ukradené herní účty mohly dosáhnout 10 až 15 USD;
- malware na zakázku se pohyboval mezi 12 až 3 500 USD;
- 1 000 followerů na sociálních sítích by stálo 2 až 12 USD;
- ukradené cloudové účty byly hodnoceny 7 až 8 USD;
- 1 milion verifikovaných e-mailů pro rozesílání spamu stálo pouze 70 až 150 USD; a

- registrované a aktivované SIM karty pro ruské mobilní telefony byly ceněny na 100 USD (str. 89).

Ponemon Institute (2016) uskutečnil rozhovory s 304 experty na hrozby, kteří sídlili v USA, UK a Německu a považovali se za:

- dobře obeznámené se současnými metodami hackingu;
- zkušené v úspěšném pronikání do počítačových systémů; a
- součást hackerské komunity.

Většina těchto expertů (69 %) uvedla, že primární motivací pro kybernetické útoky jsou finanční důvody. Odhadovali, že si útočníci vydělali ročně 28 744 USD, pouze čtvrtinu roční mzdy odborníka na kybernetickou bezpečnost. Vnímali útočníky jako oportunisty, kteří si vybírají nejsnadnější cíl; 72 % se domnívalo, že útočníci nebudou ztrácet čas s útoky, které neposkytnou cenné informace rychle. Podobně se velká část expertů (69 %) domnívá, že hackeři upustí od dalšího útoku, narazí-li na silnou obranu organizace. Typický útočník může strávit plánováním a realizací útoku proti organizaci s běžnou bezpečnostní infrastrukturou přibližně 70 hodin, ale proti organizaci s výbornou IT infrastrukturou při obdobném útoku také více než 6 dní (147 hodin).

Znepokojujícím zjištěním bylo, že dle přesvědčení poloviny expertů celkové náklady útočníků na úspěšné útoky i čas potřebný k jejich plánování a realizaci klesly, což by jen zvýšilo množství útoků proti různým průmyslovým odvětvím. Většina z nich soudila, že množství využitelných slabin a exploitů i schopnosti hackerů se zvyšují. Ponemon Institute se domnívá, že investování do účinnosti bezpečnostních opatření by mohlo výrazně snížit úspěšnost útoků, neboť by zvýšilo míru nezbytného úsilí na straně hackerů. Podobně jako ostatní studie Ponemonu, i tato zpráva hovoří o vlastních omezeních vztahujících se k online výzkumu, včetně zkreslení v důsledku non-respondence, zkreslení oporou výběru a problémů spojených se self-reporty (str. 16).

Příloha 2: Slovník pojmů používaných ve výzkumném rámci nákladů kyberkriminality

Pojmy	Definice
Důvěra spotřebitelů/ochrana identity (např. CIFAS)	Přímé peněžní náklady a náklady příležitosti spojené s částkami, které jednotlivé osoby zaplatí společnostem poskytujícím ochranu identity a dobré pověsti.
Emoční/fyzické újmy	Přímé náklady a náklady příležitosti spojené s léčbou emočního a fyzického poškození zdraví v důsledku kybernetické viktimizace.
Kriminalita usnadněná ICT	Tradiční kriminalita, jejíž rozsah a dosah se s použitím počítačů, počítačových sítí nebo jiných forem informačních a komunikačních technologií zvyšuje. Na rozdíl od kriminality závislé na ICT může být spáchána i bez použití ICT (Home Office, 2013c).
Kriminalita závislá na ICT	Trestná činnost, kterou lze spáchat pouze s použitím počítače, počítačových sítí nebo jiných forem informačních a komunikačních technologií, tzv. "čistá" kybernetická kriminalita (Home Office, 2013c).
Náklady dopadu kybernetické kriminality	Náklady vznikající následkem kriminality (např. peněžní ztráta nebo poškození IT systémů). Nad těmito náklady máte jen malou nebo žádnou kontrolu.
Náklady na anticipaci či prevenci kybernetické kriminality	Opatření za účelem snížení rizika nebo pravděpodobnosti viktimizace zahrnující obranné a bezpečnostní návyky (vynaložené např. na antivirus nebo kurz počítačové bezpečnosti).
Náklady příležitosti	Každý výběr má náklady příležitosti; předpokládá se, že prostředky lze vždy použít i jinak. Jestliže jsou použity na A místo na B, hodnota B představuje náklady příležitosti. Např. pokud má firma možnost investovat 100 liber a chce je investovat do softwaru anebo do marketingu v dané ceně, musí si mezi nimi vybrat. Zvolí-li software, hodnota marketingu je nákladem příležitosti. Náklady příležitosti budou vyjádřeny jako tržní cena věcí typu pořízení antivirového softwaru nebo zaměstnání nové osoby na opravu poškozených souborů, protože se jedná o nové finanční transakce.
Náklady vyjádřitelné v penězích	Dopady, které lze jednoduše vyjádřit v penězích, tzn. kde mohou být náklady vyčísleny pomocí tržní hodnoty/ceny (např. náklady na ukradený majetek či škodu na zařízení s určitelnou cenou).
Náklady vynaložené v reakci na kybernetickou kriminalitu	Náklady vyvstávající na základě vašeho rozhodnutí, jak odpovědět na konkrétní událost (např. zapojení orgánů činných v trestním řízení). Nad těmito náklady máte větší kontrolu, neboť máte více možností, jak se rozhodnout. Nezahrnuje obecné reakce na kybernetickou kriminalitu vůbec (např. informační kampaň vlády jako obecná reakce na kybernetickou kriminalitu).
Náklady, které nelze vyjádřit v penězích	Dopady, které nelze jednoduše vyjádřit v penězích, tzn. neexistuje jejich tržní hodnota/cena, a musí být proto odhadnuty s použitím jiných dat (např. dobrá pověst firmy, emoční nebo fyzické újmy).
Náprava úvěrové historie/ úvěrového skóre	Přímé peněžní náklady a čas vynaložené jednotlivci, firmami a státními orgány na nápravu úvěrové historie/ úvěrového skóre poškozených v důsledku podvodného použití osobních údajů.
Narušení obchodní činnosti (včetně ztráty produkce)	Ztráta tržeb v průběhu a bezprostředně po útoku způsobená neschopností subjektu normálně fungovat (např. nefunkční či zpomalené webové stránky v důsledku DDoS útoku, přerušení online prodeje). Zahrnuje náklady spojené se sníženou produktivitou zaměstnanců v důsledku útoku.
Obava/znepokojení z kybernetické kriminality	Obava/znepokojení z kybernetické kriminality s negativním emoční nebo fyzickým dopadem na kvalitu života.
Ochranný zabezpečovací software/ produkty	Přímé náklady na antivirové a jiné programy a produkty pro počítačovou bezpečnost a náklady příležitosti, které by mohli jednotlivec, společnost či státní subjekt vynaložit na jiné produkty, výnosnější nebo potřebnější. Zahrnuty jsou i přímé náklady na záplatovací software, který snižuje zranitelnost. Jsou zde též náklady příležitosti, neboť finanční prostředky a čas/produktivita mohly být vynaloženy na jiné záležitosti.

Pojmy	Definice
Online krádež, podvody s finančními prostředky	Množství finančních prostředků odčerpaných krádeží či podvodem. Zahrnují i náklady příležitosti, neboť tyto prostředky mohly být investovány do rozvoje společnosti.
Oznamování/dokumentace incidentů	Přímé náklady a náklady příležitosti pro spotřebitele, společnosti a nevládní agentury, které shromažďují a dokumentují případy kybernetických útoků na různé subjekty. To zahrnuje i pátrání po příčině, čas spotřebovaný na realizaci vnitřních procesů/požadavků společnosti a subjektů, jimž se incidenty ohlašují atd.
Poškození dobré pověsti nebo značky	Ztráty spojené se snížením dobré pověsti firmy nebo její obchodní značky v důsledku kybernetického útoku. Zahrnuje (nejen) ztrátu hodnoty společnosti (např. na burze), budoucí ztrátu příjmů, ztrátu očekávání a důvěry ve značku/firmu. Zahrnuje také poškození reputace a ztrátu očekávání/důvěry ve vládu a prosazení zákona.
Poškození zařízení/ infrastruktury	Přímé náklady na odstranění škod na zařízení/IT infrastruktuře.
Právní poradenství, PR a podobné výdaje	Peněžní náklady a náklady příležitosti na právní poradenství, PR poradenství a podobné výdaje (např. cestovní), které spotřebitelé, společnosti, státní úřady a jiné subjekty vynaloží v reakci na kybernetický trestný čin (např. najmutí právníka nebo PR týmu pro vyřešení sporů nebo důsledků negativní publicity způsobené kybernetickou kriminalitou).
Prosazování zákona a narušení protiprávní činnosti	Náklady na prosazení zákona s cílem předejít, narušit a vyšetřit kybernetické trestné činy. To zahrnuje činnost NCA, Regional Organised Crime Units[39] a místních oddělení policie. Příklady zahrnují (nejen) zrušení webových stránek, laboratoře, digitální forenzní software, každodení náklady na vyšetřovatele/vyšetřování. Obsaženy jsou i náklady příležitosti, neboť: 1) policisté mohou použít svůj čas a zdroje proti jiným formám trestné činnosti; a 2) vláda poskytující zdroje by je mohla použít na jiné priority.
Prověření bilanční historie/ záznamů	Přímé penežní náklady jednotlivců, společností a státních subjektů vynaložené na prověření bilanční historie/ záznamů za účelem časné identifikace podvodného zneužití osobních údajů. Zahrnuje rovněž náklady příležitosti ve vztahu k času vynaloženému jednotlivci, společnostmi a státními subjekty, který mohl být využit produktivněji.
Prověřování personálu a dodavatelů z hlediska bezpečnosti	Přímé náklady vynaložené firmami, organizacemi aj. subjekty na prověření jednotlivců a dodavatelů z hlediska bezpečnosti, ať už prověřování provádí samotný subjekt nebo zaplatí za prověření externí společnosti. Zahrnuje náklady příležitosti, neboť peněžní prostředky a čas mohly být použity daným subjektem jinak. Mimo to jsou zde i náklady příležitosti na straně prověřované osoby či subjektu s ohledem na ztrátu produktivity nebo zpožděné výnosy v důsledku prověřování.
Příprava a tvorba nové legislativy	Náklady na tvorbu nové legislativy, týkající se kybernetické kriminality. Jde především o náklady příležitosti, neboť čas a další zdroje by mohly být vynaloženy na řešení jiných sociálních záležitostí.
Realizace národních kampaní na zvyšování povědomí/ochrany	Přímé náklady národních kampaní zvyšujících povědomí /ochranu, které jsou iniciované vládou a/nebo jinými orgány a navržené primárně za účelem snížení viktimizace veřejnosti obecně, spotřebitelů, ale i podnikatelských subjektů (např. Cyber Streetwise, GetSafeOnline). Jsou zahrnuty mezi náklady vynaloženými v reakci, protože bývají obvykle realizovány následně po kyber viktimizaci a mají za cíl předejít dalším incidentům v budoucnu. Obsahují také náklady příležitosti, neboť finanční prostředky a čas potřebné pro tyto kampaně mohly být použity na jiné záležitosti.

39 Regionální policejní jednotky UK určené pro boj se závažným a organizovaným zločinem – pozn. překl.

Pojmy	Definice
Shromažďování údajů a sestavování statistik kybernetické kriminality	Přímé náklady policie a bezpečnostních složek (místní, národní) na shromažďování, sestavování a hlášení statistických údajů o různých formách kybernetické kriminality. To zahrnuje i náklady Action Fraud coby národního ohlašovacího centra pro kybernetickou kriminalitu a podvody. Jde též o náklady příležitosti, neboť dané orgány by mohly použít finanční prostředky a čas ke sběru a analýze statistik k jiným trestným činům nebo k řešení jiných priorit vůbec. Zahrnuty jsou i přímé náklady jiných úřadů (např. vládních jako Office for National Statistics) na shromažďování, sestavování a hlášení statistických údajů o různých formách kybernetické kriminality. Dále taktéž jejich náklady příležitosti, neboť by mohly použít svůj čas a finanční prostředky na řešení jiných priorit.
Sledování zabezpečení třetí strany	Peněžní náklady na sledování bezpečnostních opatření/ procesů třetích stran a nákladů příležitosti zahrnujících peněžní zdroje a čas, které by mohly být použity na jiné priority.
Služby na podporu obětí	Přímé náklady a náklady příležitosti finančních prostředků vynaložených vládou a podnikatelskými subjekty na podpůrné služby obětem. Mohou zahrnout i širší podporu, např. zdravotní služby pomáhající s emočními a fyzickými dopady útoku.
SME, malé a střední podniky	Malé a střední podniky: aby společnost v UK mohla být definována jako SME, musí splňovat 2 ze 3 kritérií: 1) obrat nižší než 25 milionů liber, 2) méně než 250 zaměstnanců; a 3) hrubá aktiva nižší než 12,5 milionu liber. Definice, co je SME, se liší mezi různými vládními agenturami.
Snaha vzdělávat veřejnost v nové legislativě	Přímé náklady na informování o nové legislativě (např. webové stránky, média), ale též náklady příležitosti spojené se zdroji a časem využitým na vzdělávání veřejnosti v nové legislativě, které mohly být použity jinak.
Snížení výdajů na výzkum a vývoj	Náklady vyvstalé v reakci na kybernetický útok a vyvolané neochotou firmy inovovat nebo investovat do výzkumu a vývoje, pokud nemohou zajistit, že jejich IT systémy jsou dostatečně zabezpečené, aby zabránily budoucím útokům.
Správa pojištění kybernetických rizik	Pojistné plány proti kybernetickým útokům obvykle pokrývají závazky ve vztahu k narušení bezpečnosti sítí. Náklady zahrnují pouze administrativu, vlastní pojistné náklady nikoli. (To proto, že jediné zdroje, které jsou zapojené do pojištění a představují spíše náklady pro společnost než transferovou platbu, jsou ty administrativní. Pojišťovny platí v rámci své činnosti zaměstnance, prostory a vybavení. Zdroje používané v administrativě pojišťoven představují pro společnost náklady příležitosti, neboť bez kriminality by mohly být přínosně použity jinde v ekonomice).
Stíhání kybernetických trestných činů	Přímé náklady trestního řízení (soudce, státní zástupce, obhájce ex offo), včetně vyšetřování vedeného státním zástupcem, a náklady příležitosti, neboť finanční prostředky a čas mohly být použity na jiné trestné činy.
Školení/vzdělávání realizované v přímé reakci na viktimizaci	Školení a vzdělávání, které byly realizovány/ absolvovány podnikatelskými subjekty a jednotlivci v reakci na viktimizaci kybernetickou kriminalitou (spíše než na její anticipaci).
Školení a vzdělávání v kybernetické bezpečnosti	Peněžní náklady na zajištění a realizaci školení a vzdělávání v oblasti kybernetické bezpečnosti pro zaměstnance a spotřebitele/veřejnost. Mohou zahrnout náklady na čas potřebný k získání znalostí/pochopení existujících hrozeb a osvojení si dovednosti vypořádat se s nimi. Náklady příležitosti zahrnují finanční prostředky i čas, které by mohly byt použity na jiné záležitosti či školení.
Školení soudního a právního personálu	Náklady na školení soudního personálu aj. osob podílejících se na trestním řízení (např. soudci, státní zástupci, veřejní obhájci) o kybernetické kriminalitě (např. co to je, prevalence, právní předpisy). Zahrnuje náklady příležitosti, neboť peněžní prostředky a čas mohly být použity na jiné formy školení nebo na jiné státní priority.
Uvěznění pachatelů kybernetické kriminality	Přímé náklady na uvěznění pachatelů usvědčených z kybernetických trestných činů a náklady příležitosti, neboť použité zdroje mohly být využity na uvěznění jiných typů pachatelů nebo na jiné priority státu.
Velké obchodní podniky (LBE)	Velké obchodní podniky: subjekty byznysu větší, než vyhovují kritériím pro malé a střední podniky. Viz definice SME.

Pojmy	Definice
Vliv zvýšených bezpečnostních opatření na uživatele a obvyklé používání	Ztráta produktivity uživatele (např. zaměstnance, jednotlivce) v důsledku zvýšených bezpečnostních opatření.
Výcvik policejních vyšetřovatelů a důstojníků	Náklady na školení vyšetřovatelů a důstojníků v oblasti správné reakce a vyšetřování různých forem kybernetické kriminality. Zahrnuje rovněž náklady příležitosti, neboť peněžní prostředky a čas mohly být využity policejními složkami jinak, včetně jiného výcviku.
Výdaje na clean-up	Přímé náklady a náklady příležitosti spojené s vynaloženým časem a penězi na vyřešení bezpečnostních problémů a škod a/nebo odhalení příčin útoku. Mohou vzniknout na mnoha stranách, od jednotlivců po subjekty byznysu, poskytovatele internetových služeb nebo společnosti poskytující bezpečnostní služby.
Vyhýbání se internetu a/nebo jiným technologiím (mezi ne-uživateli)	Strach z kybernetické kriminality (např. případy zveřejněné v médiích) může vyvolat obavy z viktimizace mezi osobami, které internet či jiné technologie již tak příliš nevyužívají. To je může přimět k tomu, že se jim budou vyhýbat úplně a uchýlí se výlučně k tradičním offline technologiím.
Zavádění kyber bezpečnostních návyků	Náklady příležitosti na čas strávený zaváděním kyber bezpečnostních návyků jako aktualizace softwaru nebo prověřování autenticity emailů/ webových stránek. Není zahrnut čas spojený se školením a/nebo vzděláváním jednotlivců v oblasti kybernetické ochrany.
Zavedení nových/dalších technologií	Náklady na nové technologie snižující kybernetickou kriminalitu jako jsou podvody (např. EMV kreditní karty, zabezpečený email). I zde existují náklady příležitosti, neboť peněžní prostředky mohly být použity na jiné priority.
Změna ISP a poskytovatelů zabezpečení nebo produktů	Přímé náklady vzniklé změnou poskytovatele internetového připojení (ISP), poskytovatelů zabezpečení nebo jiných produktů týkajících se bezpečnosti (např. administrativní poplatky, zvýšená cena produktu) a náklady příležitosti zahrnující čas potřebný pro implementaci změn.
Změna ISP a poskytovatelů zabezpečení nebo produktů jako přímá reakce na viktimizaci	Přímé náklady vzniklé změnou poskytovatele internetového připojení (ISP), poskytovatelů zabezpečení nebo jiných produktů týkajících se bezpečnosti (např. administrativní poplatky, zvýšená cena produktu) a náklady příležitosti zahrnující čas potřebný pro implementaci změn. Vyskytují se jako přímá reakce na viktimizaci kybernetickým trestným činem spíše než v jeho anticipaci.
Zpochybněné transakce	Peněžní náklady a náklady příležitosti zahrnující čas a právní poplatky vynaložené jednotlivci a společnostmi na prošetření a vyřešení zpochybněných nároků spotřebitelů.
Ztráta hodnoty DV/obchodně citlivých informací	Hodnota duševního vlastnictví nebo obchodně citlivých informací zcizených během kybernetického útoku. Může být odhadnuta jako hodnota duševního vlastnictví nebo obchodně citlivé informace na volném trhu, ale také jako poškození konkurenceschopnosti firmy v důsledku této ztráty.
Zvýšení nákladů na probační systém	Přímé náklady související s dohledem nad pachateli kybernetické kriminality odsouzenými k podmíněnému trestu. Dále náklady příležitosti, neboť finanční prostředky i čas by mohly být využity k monitorování jiných typů pachatelů nebo vynaloženy na jiné priority státu.
Zvýšené/lépe vynaložené náklady na IT jako přímá reakce na viktimizaci	Zvýšené peněžní náklady a náklady příležitosti na IT nad rámec běžných provozních procesů v důsledku kybernetické kriminality. Zahrnuje též lepší vynaložení výdajů, např. na zařízení/technologie/ ochranný software. Jde o věci zavedené v přímé reakci na viktimizaci kybernetickou trestnou činností spíše, než na její anticipaci.

Příloha 3: Návrh nástrojů pro zjišťování hodnoty dobré pověsti podnikatelských subjektů

Následující navržené kvantitativní nástroje jsou určeny na přidání do dotazníků pro obchodní subjekty, aby pomohly kvantifikovat jejich hodnotu dobré pověsti. To pomůže výzkumným pracovníkům odhadnout dopad kybernetických útoků na dobrou pověst v podnikání. Otázky by před použitím při sběru dat vyžadovaly další kognitivní testování a úpravy, aby napomohly v budoucích velkých studiích měřit náklady spojené s kybernetickou kriminalitou.

Otázky pro podnikatelské subjekty, které mají zkušenost s kybernetickou kriminalitou

1) **Počet případů, kdy se setkali s určitým typem kybernetické trestné činnosti** – je to důležité, protože to udává hladinu tolerance veřejnosti/zákazníka vůči kybernetické kriminalitě.

O1. *[ZAŘADIT VŠECHNY]*

Kolikrát se v posledních 12 měsících (pokud vůbec) vaše firma setkala s následujícími typy kybernetického útoku?

- **A.** Napadení virem nebo škodlivým softwarem (škodlivý software)
- **B.** Neoprávněný přístup k datům nebo informaci, které jsou v majetku firmy (hacking/průnik do počítače)
- **C.** Narušení webových stránek vaší firmy (DDOS útoky)
- **D.** Neoprávněná úprava obsahu webových stránek vaší firmy (web defacement)
- **E.** Neoprávněné použití obchodních informací nebo účtu k získání peněz nebo koupi zboží či služeb bez autorizace vaší firmy (podvod/krádež)
- **F.** Podvodné vylákání peněz nebo zboží (podvod/krádež)
- **G.** Krádež duševního vlastnictví (krádež duševního vlastnictví)
- **H.** Jiné (prosím specifikujte)
- **I.** Nic z uvedeného
- **J.** Nevím *(VOLITELNÉ)*

2) **Povaha kybernetické trestné činnosti, k níž došlo** – jde o souhrnnou odpověď mapující kategorie vážící se k rámci nákladů spojených s kybernetickou kriminalitou.

Povaha kybernetické kriminality je důležitá při určování dopadu trestné činnosti na podnikatelský subjekt a umožní vyhodnotit potenciální dopady podle typu kybernetické trestné činnosti.

O2. *[DOTAZ NA ZKUŠENOST S VÍCE NEŽ JEDNÍM TYPEM KYBERNETICKÉ TRESTNÉ ČINNOSTI]*

Která z následujících odpovědí nejlépe odpovídá **poslednímu** případu kybernetického útoku, který zasáhl vaši firmu?

- **A.** Napadení virem nebo škodlivým softwarem (škodlivý software)

B. Neoprávněný přístup k datům nebo informaci, které jsou v majetku firmy (hacking/průnik do počítače)
C. Narušení webových stránek vaší firmy (DDOS útoky)
D. Neoprávněná úprava obsahu webových stránek vaší firmy (zkreslení webových stránek)
E. Neoprávněné použití obchodních informací nebo účtu k získání peněz nebo koupi zboží či služeb bez autorizace vaší firmy (podvod/krádež)
F. Podvodné vylákání peněz nebo zboží (podvod/krádež)
G. Krádež duševního vlastnictví (krádež duševního vlastnictví)
H. Jiné (prosím specifikujte)
I. Nic z uvedeného
J. Nevím *(VOLITELNÉ)*

O2b. *[DOTAZ NA ZKUŠENOST S VÍCE NEŽ JEDNÍM TYPEM KYBERNETICKÉ TRESTNÉ ČINNOSTI]*

Která z následujících odpovědí nejlépe popisuje **nejzávažnější** kybernetický útok, kterému byla vystavena vaše společnost?

A. Napadení virem nebo škodlivým softwarem (škodlivý software)
B. Neoprávněný přístup k datům nebo informaci, které jsou v majetku firmy (hacking/průnik do počítače)
C. Narušení webových stránek vaší firmy (DDOS útoky)
D. Neoprávněná úprava obsahu webových stránek vaší firmy (zkreslení webových stránek)
E. Neoprávněné použití obchodních informací nebo účtu k získání peněz nebo koupi zboží či služeb bez autorizace vaší firmy (podvod/krádež)
F. Podvodné vylákání peněz nebo zboží (podvod/krádež)
G. Krádež duševního vlastnictví (krádež duševního vlastnictví)
H. Jiné (prosím specifikujte)
I. Nic z uvedeného
J. Nevím (VOLITELNÉ)

[POKUD SE POSLEDNÍ A NEJZÁVAŽNĚJŠÍ ÚTOK LIŠÍ, MĚLY BY BÝT POLOŽENY VŠECHNY NÁSLEDUJÍCÍ OTÁZKY VE VZTAHU K POSLEDNÍMU ÚTOKU A POTÉ K NEJZÁVAŽNĚJŠÍMU ÚTOKU]

3) Rozsah publicity kybernetického útoku

O3. *[ZAŘADIT VŠECHNY]*

Jak byste nejlépe popsal/a míru publicity **posledního** kybernetického útoku, kterému byla vystavena vaše firma?

- Podrobné zpravodajství
- Omezená mediální publicita
- Žádná mediální publicita
- Nevím *(VOLITELNÉ)*

Jak nejlépe byste popsal/a míru publicity **nejzávažnějšího** kybernetického útoku, který postihl vaši firmu?

O4. *[ZAŘADIT VŠECHNY]*

Pokud je vám známo, které z následujících osob si byly vědomy **posledního** kybernetického útoku?

A. Nikdo kromě několika nejvýše postavených pracovníků ve firmě
B. Malý počet zaměstnanců
C. Velký počet zaměstnanců firmy
D. Obchodní společníci a potenciální partneři
E. Investoři, poskytovatelé peněžních prostředků a akcionáři
F. Konkurence
G. Malý počet existujících nebo potenciálních zákazníků
H. Velký počet existujících nebo potenciálních zákazníků
I. Veřejnost
J. (prosím specifikujte)
K. Nevím *(VOLITELNÉ)*

Pokud je vám známo, které z následujících osob si byly vědomy **nejzávažnějšího** kybernetického útoku?

4) Úroveň dopadu kybernetické trestné činnosti

O5. *[ZAŘADIT VŠECHNY]*

Získal **poslední** kybernetický útok přístup k nějakým důvěrným datům?
1. Ano
2. Ne
3. Nevím

Získal **nejzávažnější** kybernetický útok přístup k nějakým důvěrným datům?

O6. *[ZAŘADIT, JESTLIŽE O4=G NEBO O4=H]*

Pokud je vám známo, utrpěl některý z vašich zákazníků jakoukoliv finanční ztrátu v důsledku **posledního** kybernetického útoku, kterému byla vaše firma vystavena?
1. Ano
2. Ne
3. Nevím

Pokud je vám známo, utrpěl některý z vašich zákazníků jakoukoliv finanční ztrátu v důsledku **nejzávažnějšího** kybernetického útoku, kterému byla vaše firma vystavena?

5) Vliv na dobrou pověst

O7. *[ZAŘADIT VŠECHNY]*

Jaký dopad (pokud vůbec nějaký) měl podle vašeho názoru **poslední** kybernetický útok na míru důvěry[40] stávajících zákazníků ve vaši firmu?

1. Hodně zvýšená
2. Trochu zvýšená
3. Žádná změna
4. Trochu snížená
5. Hodně snížená
6. Nevím *(VOLITELNÉ)*

Jaký dopad (pokud vůbec nějaký) měl podle vašeho názoru **nejzávažnější** kybernetický útok na míru důvěry stávajících zákazníků ve vaší firmu?

O8. Jak důležité je podle vašeho názoru pro vaše zákazníky kybernetické zabezpečení vaší firmy?

1. Velmi důležité
2. Docela důležité
3. Nepříliš důležité
4. Nedůležité
5. Nevím *(VOLITELNÉ)*

O9. Jak byla podle vás poškozena dobrá pověst vaší firmy **posledním** kybernetickým útokem?

1. Hodně
2. Do určité míry
3. Vůbec
4. Nevím *(VOLITELNÉ)*

Jak byla podle vás poškozena dobrá pověst vaší firmy **nejzávažnějším** kybernetickým útokem?

Odhad nákladů

O9. *[ZAŘADIT VŠECHNY]*

Rád bych se zeptal na náklady spojené s jakýmkoli poškozením dobré pověsti vaší firmy v důsledku **posledního** kybernetického útoku. V jaké výši byste odhadl/a tyto náklady z hlediska ztráty příjmů, přímých nákladů spojených s řešením útoku a veškerými náklady z hlediska času potřebného pro vypořádání se s útokem?

Nejprve, v jaké výši byste odhadl/a náklady spojené s poškozením dobré pověsti vaší firmy z hlediska ztráty příjmů?

40 „Důvěra" použita namísto „dobré pověsti".

Ztráta příjmů by mohla zahrnout jakékoli omezení stávající anebo potenciální obchodní činnosti.

Uveďte prosím váš nejlepší odhad.
[VLOŽTE ODHAD]
Nevím

Jaká byla ztráta příjmů spojená s poškozením dobré pověsti vaší firmy v důsledku **nejzávažnějšího** útoku?

[VLOŽTE ODHAD]

O10. *[ZAŘADIT VŠECHNY]*

V jaké výši byste odhadl/a náklady spojené s poškozením dobré pověsti vaší firmy z hlediska přímých nákladů na řešení **posledního** útoku?

Přímé náklady by mohly zahrnout:
- IT náklady spojené s řešením útoku
- Jiné náklady na zvládnutí útoku
- Právní poplatky
- Slevy nebo náhrady zákazníkům poskytnuté jako kompenzace ve vztahu k útoku

Uveďte prosím váš nejlepší odhad.
[VLOŽTE ODHAD]
Nevím

V jaké výši byste odhadl/a náklady spojené s poškozením dobré pověsti vaší firmy z hlediska přímých nákladů na řešení **nejvážnějšího** útoku?

[VLOŽTE ODHAD]

O11. *[ZAŘADIT VŠECHNY]*

V jaké výši byste odhadl/a náklady spojené s poškozením dobré pověsti vaší firmy z hlediska času potřebného pro vypořádání se s **posledním** útokem?

Náklady na čas by zahrnuly čas strávený zaměstnanci firmy na vypořádání se s útokem.

Uveďte prosím váš nejlepší odhad.
[VLOŽTE ODHAD]
Nevím

V jaké výši byste odhadl/a náklady spojené s poškozením dobré pověsti vaší firmy z hlediska času potřebného pro vypořádání se s **nejvážnějším** útokem?

[VLOŽTE ODHAD]

O12. *[ZAŘADIT, JESTLIŽE SE JEDNÁ O AKCIOVOU SPOLEČNOST]*

V jaké výši byste odhadl/a náklady spojené s poškozením dobré pověsti vaší firmy z hlediska snížení ceny akcií ve vztahu k **poslednímu** útoku?

Uveďte prosím váš nejlepší odhad.
[VLOŽTE ODHAD]
Nevím

V jaké výši byste odhadl/a náklady spojené s poškozením dobré pověsti vaší firmy z hlediska snížení ceny akcií ve vztahu k **nejvážnějšímu** útoku?

[VLOŽTE ODHAD]

O13. *[ZAŘADIT VŠECHNY]*

V jaké výši byste odhadl/a náklady spojené s poškozením dobré pověsti vaší firmy z hlediska jakýchkoli dalších nákladů potřebných na vypořádání se s **posledním** útokem?

Uveďte prosím váš nejlepší odhad.
[VLOŽTE ODHAD]
Nevím

V jaké výši byste odhadl/a náklady spojené s poškozením dobré pověsti vaší firmy z hlediska jakýchkoli dalších nákladů potřebných na vypořádání se s **nejzávažnějším** útokem?

[VLOŽTE ODHAD]

Alternativní návrh v1

V průběhu projektu byly zvažovány dva návrhy. Pro určení, který návrh je pro budoucí výzkum zabývající se náklady spojenými s kybernetickou kriminalitou vhodnější, je nutné další testování a vývoj.

Rád bych se vás zeptal na náklady spojené s poškozením dobré pověsti vaší firmy v důsledku útoku. V jaké výši byste odhadl/a tyto náklady ve vztahu mezi následujícími možnostmi a poškozením dobré pověsti vaší firmy?

- Ztráta příjmů (např. omezení stávající nebo potenciální obchodní činnosti způsobená publicitou / povědomím o prolomení zabezpečení)?
  - *[VLOŽTE ODHAD]*
  - Nevím

- Náklady vyplývající ze ztráty podpory investora nebo poskytovatele peněžních prostředků v důsledku publicity / povědomí o prolomení zabezpečení?
  - *[VLOŽTE ODHAD]*
  - Nevím

- Náklady na vypořádání se s útokem (např. poplatky za PR; čas zaměstnanců věnovaný na služby pro zákazníky, poskytování informací o útoku nebo vyřizování stížností a dotazů)?
  - *[VLOŽTE ODHAD]*
  - Nevím

- Náklady na "dobrovolné" kompenzační platby nebo slevy pro zákazníky?
  - *[VLOŽTE ODHAD]*
  - Nevím

- *[JESTLIŽE SE JEDNÁ O AKCIOVOU SPOLEČNOST]* Snížení ceny akcií?
  - *[VLOŽTE ODHAD]*
  - Nevím

- Jakékoli jiné náklady ve spojení s dobrou pověstí firmy?
  - *[VLOŽTE ODHAD]*
  - Nevím

Alternativní návrh v2

V průběhu projektu byly zvažovány dva návrhy. Tento druhý návrh by mohl být použit místo prvního. Pro určení, který návrh je pro budoucí výzkum zabývající se náklady spojenými s kybernetickou kriminalitou vhodnější, je nutné další testování a vývoj.

Rád bych se vás zeptal na náklady spojené s poškozením **dobré pověsti** vaší firmy v důsledku útoku. V jaké výši byste odhadl/a tyto náklady ve vztahu mezi následujícími možnostmi a poškozením dobré pověsti vaší firmy?

- Ztráta příjmů (např. omezení stávající nebo potenciální obchodní činnosti způsobená publicitou / povědomím o prolomení zabezpečení) nebo ztráty investic v důsledku povědomí o prolomení zabezpečení?
  - *[VLOŽTE ODHAD]*
  - Nevím

- Náklady na vypořádání se s útokem (např. poplatky za PR; čas zaměstnanců věnovaný na služby pro zákazníky, poskytování informací o útoku nebo vyřizování stížností a dotazů, včetně jakýchkoliv kompenzačních plateb)?
  - *[VLOŽTE ODHAD]*
  - Nevím

- Jakékoli jiné náklady ve spojení s dobrou pověstí firmy?
  - *[VLOŽTE ODHAD]*
  - Nevím

Příloha 4: Podrobnější publikace vztahující se ke studiím, které pro tuto zprávu vybrala Pracovní skupina

Furnell, S. (2016). „*The Evolving Landscape of Technology-Dependent Crime*", in The Routledge Handbook of Technology, Crime and Justice. M. R. McGuire and T. J. Holt (Eds), Routledge International Handbooks. Dostupné na: https://www.routledge.com/The-Routledge-Handbook-of-Technology-Crime-and-Justice/McGuire-Holt/p/book/9781138820135

Furnell, S., Emm, D. and Papadaki, M. (2015). „*The challenge of measuring cyber- dependent crimes*", Computer Fraud and Security, October 2015, str. 5-12. Dostupné na: http://www.sciencedirect.com/science/article/pii/S1361372315300932

Furnell, S. (2015). „*Getting the measure of cyber crime?*" University of Oxford, 5th June 2015. Dostupné na: https://itunes.apple.com/us/podcast/getting-measure- cybercrime/id402420124?i=1000355139549 & mt=2

Holt, T. J., Smirnova, O. and Chua, Y. T. (2016) „Exploring and estimating the revenues and profits of participants in stolen data markets", *Deviant Behavior,* 37 (4) str. 353–367.

Smirnova, O. and Holt, T. J. (2017). Examining the geographic distribution of victim nations in stolen data markets. *American Behavioral Scientist* 61(11) str. 1403-1426.

Příloha 5: Výzkumné zadání Pracovní skupiny

VÝZKUMNÉ ZADÁNÍ

1.0 Kontext

1.1 Pracovní skupina byla zřízena, aby vyšla vstříc požadavku lepšího porozumění rozsahu a nákladům kyberkriminality nastíněnému v Home Office Serious and Organised Crime Strategy.[41] Strategie si je vědoma obtížnosti úkolu poskytnout přesné odhady a uvádí:
„Soudě podle omezených dostupných důkazů představují náklady spojené s kybernetickou kriminalitou v UK každoročně pravděpodobně nejméně několik miliard liber. Home Office proto zřizuje novou externí Pracovní skupinu, aby zlepšila kvalitu dat v této oblasti." (Home Office, 2013a)

1.2 Před zformulováním Strategie vyjádřil obavu z nedostatku přesných a aktuálních číselných údajů o škále a nákladech spojených s kybernetickou kriminalitou rovněž Home Affairs Select Committee (HASC), který doporučil zřízení externí skupiny zahrnující průmysl a akademickou sféru, která by zkvalitnila takové odhady.

1.3 Lepší porozumění prevalenci a nákladům spojených s kybernetickou kriminalitou by pomohlo:
- pochopit povahu hrozby představované kybernetickou kriminalitou a jak se tato hrozba mění v čase;
- zvýšit povědomí o kybernetické kriminalitě při prosazování práva a zajistit, aby byly zdroje zacíleny na prioritní typy trestných činů; a
- zajistit, aby byly preventivní a osvětové aktivity směrovány na ty jednotlivce a podnikatelské subjekty, které jsou zranitelnější.

1.4 Obecně se Pracovní skupina zaměřuje na:
- kategorie, do kterých spadají různé náklady (např. anticipaci, přímé náklady nebo reakce na kyberkriminalitu aj.); a
- nejvíce postižené (např. které oblasti podnikání, kteří jedinci).

2.0 Úloha Pracovní skupiny

2.1 Úlohou Pracovní skupiny je řídit a provádět nezbytnou činnost s cílem zlepšit odhady sociálních i ekonomických nákladů spojených s kybernetickou kriminalitou.

2.2 Zahrnuje to činnost usilující o lepší porozumění a měření prevalence a/nebo incidence kybernetické kriminality, které jsou pro zlepšení odhadů nákladů nezbytné.

2.3 Ačkoliv je finanční aspekt důležitý, náplň práce Pracovní skupiny zahrnuje rovněž činnost usilující o lepší porozumění tomu, jak měřit širší újmy a dopady kybernetické kriminality, které nejsou finančního charakteru.

41 Strategie pro boj se závažnou a organizovanou kriminalitou, dále jen „Strategie" – pozn. překl.

2.4 Pracovní skupina zejména:

- načrtne škálu a typy kybernetické trestné činnosti, které mají nejvyšší prioritu a/nebo jsou nejlépe použitelné pro provádění odhadů nákladů;
- nalezne shodu ohledně nejlepších dostupných dat pro odhadování nákladů;
- identifikuje a doplní základní údaje o prevalenci a incidenci, které jsou vyžadovány pro kalkulaci nákladů;
- vyvine odborný a opakovaně použitelný model pro odhadování nákladů spojených s kybernetickou kriminalitou, na kterém bude panovat shoda; a
- bude monitorovat pokrok a zlepšovat odhady v průběhu času.

2.5 Pracovní skupina bude zodpovědná za:

- vytvoření a vedení pracovních programů pro vhodné pracovní oblasti (viz níže);
- přípravu pracovních plánů na období 2014/15 a 2015/16;
  poradenství k prioritám finanční podpory různých projektů; a
- monitorování pokroku a výstupů.

3.0 Náplň práce

3.1 Náplň práce Pracovní skupiny zahrnuje jakékoli formy kybernetické kriminality, tak jak je definuje Serious and Organised Crime Strategy. Tedy:

- kriminalita závislá na ICT [např. počítačové viry a jiný malware, hacking, odmítnutí služby (DoS) nebo distribuované odmítnutí služby (DDoS)];
- kriminalita usnadněná ICT (např. podvod usnadnění díky použití ICT, krádež dat).

3.2 Nezahrnuje proto:

- online kriminalitu/zneužití, kde internet slouží pouze jako médium pro komunkaci (např. sexuální obtěžování online, stalking, trestné činy z nenávisti); sexuální vykořisťování dětí;
- online terorismus/extremismus;
- kybernetické útoky na tzv. vysoké cíle[42] (např. národní infrastruktura) nebo státem sponzorovaná špionáž.

Tyto oblasti jsou pokryty jinými sekcemi Home Office nebo National Cybersecurity Programme.[43] Je však třeba zajistit, aby byly jednotlivé činnosti propojeny tak, aby všichni zúčastnění věděli o aktivitách probíhajících v jiných oblastech.

3.3 Financovat bude proto možné pouze ty projekty Pracovní skupiny, které budou týkat:

- kybernetické kriminality (jak ji definuje Serious and Organised Crime Strategy);
- měření prevalence, incidence a rozsahu jakékoli formy kybernetické kriminality;
- zjišťování finančních nákladů spojených s jakoukoli formou kybernetické trestné činnosti;
- zjišťování širších sociálních a ekonomických újem a dalších dopadů kybernetické trestné činnosti.

42 V originále high-end attack. Pozn. překl.

43 Národní program kybernetické bezpečnosti.

3.4 V rámci těchto kritérií mohou být použity různé přístupy, jak ukazují následující příklady.
- Náklady a újmy mohou být zkoumány buď z perspektivy oběti útoku (např. jednotlivci/veřejnost, subjekty byznysu, vláda, společnost jako celek), nebo pachatele (např. zisk pachatele/výnos kybernetické trestné činnosti).
- Cílem výzkumu mohou být různé typy nákladů a újem (např. náklady prevence/anticipace kybernetické kriminality; náklady dopadu kybernetické kriminality; náklady vynaložené v reakci na kybernetickou kriminalitu).
- Měření stávajících i budoucích typů kybernetické kriminality.

4.0 Členství v Pracovní skupině a její struktura

4.1 Jádrem Pracovní skupiny bude skupina akademických pracovníků a reprezentantů průmyslu a vlády. Ti budou zodpovědní za vytvoření programu a řízení činnosti Pracovní skupiny a dílčích programů/tematických oblastí. V čele Pracovní skupiny bude prof. David Delpy z Home Office Science Advisory Council.

4.2 Členové podskupin budou přizváni, aby se podíleli na jednotlivých pracovních projektech – není zde žádné konkrétní omezení jejich počtu.

4.3 Podle vývoje jednotlivých projektů mohou být přizvány k účasti jako členové podskupin i další osoby, které se dosud na projektu nepodílely. Vedoucí pracovníci tvořící jádro Pracovní skupiny by měli při plánování dílčích projektů uvážit, kdo další by v nich měl být zahrnut. Členové Pracovní skupiny mohou přizvat k účasti na jednání osoby působící mimo Pracovní skupinu, bude-li třeba jejich znalostí a odbornosti.

4.4 Osoby z vládních institucí a institucí prosazujících zákon budou pomáhat:
- vést obecný směr činnosti:
- vyjednávat přístup k datům a informacím vyžadovaným pro řešení projektů; a
- zajišťovat včasnost a relevantnost požadovaných výstupů.

4.5 Finanční zajištění poskytuje National Cybersecurity Programme (NCSP).

5.0 Řízení

5.1 Pracovní skupina se zřizuje pod záštitou Home Office Science Advisory Council (HOSAC), nezávislé poradní komise poskytující poradenství vrchnímu vědeckému poradci Home Office[44] ve věci vědeckých záležitostí.

5.2 Začlenění Pracovní skupiny do HOSAC podtrhuje:
- význam problematiky pro HOSAC a Home Office; a
- důležitost použití spolehlivých analytických přístupů pro porozumění problému.

44 Home Office Chief Scientific Adviser – pozn. překl.

5.3 Přestože se formálně nejedná o podskupinu, HOSAC může dle potřeby požadovat aktuální informace o její činnosti. Členové Pracovní skupiny by měli při podávání takových zpráv poskytnout součinnost.

5.4 Vedoucí pracovníci pro jednotlivé projekty budou na každém zasedání celé Pracovní skupiny referovat o pokroku a výsledcích svých projektů (s ohledem na pracovní plán) a žádat o její souhlas s pracovním plánem, klíčovými rozhodnutími a doporučeními.

6.0 Výstupy

6.1 V rámci pracovního programu bude realizována řada krátkodobých i déle probíhajících projektů. Ačkoliv nemusí být možné pokrýt každý aspekt nákladů, bude usilováno o pokrytí škály zájmů/oblastí. Bude usilováno o to, aby pracovní programy zahrnuly škálu zájmů/oblastí, ačkoli pravděpodobně nebude možné pokrýt všechny aspekty nákladů. Financovány mohou být i projekty mimo uvedený seznam zájmů Pracovní skupiny, pokud jejich poznatky v kombinaci s ostatními umožní lepší měření prevalence a nákladů.

6.2 Po dobu působení Pracovní skupiny (tj. během roku 2015) budou podávány krátké průběžné zprávy s výsledky z dílčích projektů. Tyto zprávy budou předávány celé Pracovní skupině.

6.3 Na konci působení Pracovní skupiny (konec března roku 2016) bude vytvořena závěrečná zpráva shrnující všechny výsledky, která poskytne finální zhodnocení prevalence, nákladů a újem; a rovněž poukáže na přetrvávající mezery ve znalostech.

7.0 Vlastnická a autorská práva k výstupům/duševnímu vlastnictví

7.1 Projekty budou financovány pomocí grantového systému, a proto nepodléhají obvyklým pravidlům, kterými se řídí projekty Home Office. Podrobnosti o autorských právech uvádí grantové dohody, včetně bodů uvedených níže v odstavcích 7.2 až 7. 4.

7.2 Příjemci grantu neodmítnou bezdůvodně udělit povolení k publikaci výsledků grantu. Povolení publikovat výsledky může být odepřeno, pokud půjde o zveřejnění dat představujících potenciální bezpečnostní riziko. K mimořádnému omezení publikování může dojít během formálního předvolebního období ('purdah')[45] od konce března do začátku května roku 2015.

7.3 Příjemci grantu musí oznámit Home Office všechny publikační záměry alespoň čtyři týdny před publikací. Home Office a Pracovní skupina k nákladům kyberkriminality musí mít náhled plánované publikace a možnost vyjádřit se k ní během této doby.

7.4 Před publikování práce musí být vyžádáno od Home Office výslovné svolení k použití názvu Home Office ve spojení s jakoukoli publicitou a písemným materiálem financo-

45 V UK mimo jiné období mezi vyhlášením voleb a oznámením jejich výsledku - pozn. překl.

vaným grantem. V publikaci musí příjemce grantu uvést, že všechny názory vyjádřené ve zprávě jsou názory jejích autorů a nutně se nekryjí se stanovisky či politikou Home Office (nebo vlády UK vůbec).

8.0 Časový rozvrh

8.1 Pracovní skupina ukončí svoji činnost na konci března 2016. V této době bude zváženo, zda má skupina ve své práci pokračovat (a zda jsou pro to dostupné finanční prostředky) nebo jestli je její práce dokončena. Jednotlivé projekty a průběžné poznatky budou zveřejňovány v průběhu období 2014/15 a 2015/16.

8.2 Vedoucí pracovníci Pracovní skupiny vytvořili první pracovní plán na období od listopadu 2014 do března 2015, odsouhlasen byl v prosinci 2014. Po schválení finančních požadavků na období 2015/16 vytvořila Pracovní skupina v březnu 2015 pracovní plán pro období 2015/16. Pracovní plány byly revidovány na každém setkání.

Příloha 6: Seznam členů Pracovní skupiny

Předseda:

- Profesor Dave Delpy, University College London and Home Office Science Advisory Council

Členové Working Group:

- Ruth Davies, Tech UK
- Ali Imanat; Financial Fraud Action UK
- Professor David Pym, University College London
- Professor Steve Furnell, Plymouth University
- Dr Tom Holt, Michigan State University, USA
- Dr Alice Hutchings, Cambridge University
- Professor David Wall, University of Leeds
- Emma Dickens, Cabinet Office
- John Flatley, Office for National Statistics
- Patrick Anderson, National Crime Agency
- Gareth Rees, National Crime Agency
- Dave Fyson, Department for Culture, Media and Sport
- Tom Ryder, National Crime Agency
- Henry Bryers, National Crime Agency
- DI Chris Felton, City of London Police

Příloha 7: Slovníček nepřekládaných pojmů

clean-up = „vyčištění", v oblasti ICT obvykle optimalizace chodu zařízení odstraněním nežádoucího softwaru a souborů (malware, nepoužívaný software atd.)

cyber-dependent crime = trestná činnost zcela závislá na použití ICT, tj. malware, DDoS atp.

cyber-enabled crime = trestná činnost usnadněná v prostředí ICT, tzn. vyskytující se i offline, avšak v online prostředí zpravidla provedená ve větší míře, s větší rychlostí, závažnějšími dopady atd. Např. sexuální vykořisťování dětí nebo obchodování s drogami

malware = škodlivý software

open web = obsah internetu mimo dark web

web defacement = "zkreslení" webových stránek, tj. neoprávněná úprava jejich původního obsahu útočníkem (změna původních dat, jejich smazání nebo vložení dat nových)

Přehled titulů vydaných v edici Institutu pro kriminologii a sociální prevenci od roku 2012

Ediční řada Studie:

2019

449 Roubalová, M., Holas, J., Kostelníková, Z. & Pešková, M. *Oběti kriminality. Poznatky z viktimizační studie.*

2018

447 Diblíková, S., Hulmáková, J., Večerka, K., Scheinost, M., Cejp, M. & Pešková, M. *Analýza trendů kriminality v České republice v roce 2017.*

446 Scheinost, M., Cejp, M., Pojman, P. & Diviák, T. *Trendy vývoje organizovaného zločinu a jeho vybraných forem.*

2017

440 Zeman, P. (ed.) *Research on Crime and Criminal Justice in the Czech Republic (selected results of research activities of IKSP in the years 2012–2015).*

441 Tomášek, J., Faridová, P., Kostelníková, Z., Přesličková, H., Rozum, J. & Zhřívalová, P. *Zaměstnání jako faktor desistence.*

443 Karabec, Z., Hulmáková, J., Vlach, J., Diblíková, S., Zeman, P. *Criminal Justice System in the Czech Republic. 3rd amended and revised edition.*

444 Budka, I. *Využití právních nástrojů pro potírání organizovaného zločinu.*

445 Diblíková, S., Hulmáková, J., Večerka, K., Scheinost, M., Karban, M., Martinková, M. *Analýza trendů kriminality v České republice v roce 2016.*

2016

431 Blatníková, Š., Faridová, P., Vranka, M. *Kriminální styly myšlení: Inventář PICT-cz.*

432 Marešová, A., Biedermanová, E., Rozum, J., Tamchyna, M. & Zhřívalová, P. *Výkon nepodmíněného trestu odnětí svobody – kriminologická analýza.*

433 Blatníková, Š. *Nebezpečnost a násilí ve vězeňském prostředí.*

435 Holas, J., Krulichová, E., Háková, L., Scheinost, M. *Regionální kriminalita a její odraz v kvalitě života obyvatel.*

437 Diblíková, S., Cejp, M., Štefunková, M., Smejkal, V. & Martinková, M. *Analýza trendů kriminality v České republice v roce 2015.*

438 Tomášek, J., Diblíková, S. & Scheinost, M. *Probace jako efektivní nástroj snižování recidivy.*

439 Rozum, J., Tomášek, J., Vlach, J. & Háková, L. *Efektivita trestní politiky z pohledu recidivy.*

2015

423 Scheinost, M., Háková, L., Rozum, J., Tomášek, J. & Vlach, J. *Trestní sankce – jejich uplatňování, vliv na recidivu a mediální obraz v televizním zpravodajství. (Teoretické a trestněpolitické aspekty reformy trestního práva v oblasti trestních sankcí III.).*

424 Marešová, A., Havel, R., Martinková, M. & Tamchyna, M. *Násilná kriminalita v nejisté době.*

425 Marešová, A., Biedermanová, E., Diblíková, S., Požár, J. & Martinková, M. *Analýza trendů kriminality v ČR v roce 2014.*
426 Zeman, P., Štefunková, M. & Trávníčková, I. *Drogová kriminalita a trestní zákoník.*
427 Večerka, K. & Štěchová, M. *Preventivní praxe po novelizaci zákona o sociálně-právní ochraně dětí.*
428 Blatníková, Š., Faridová, P. & Zeman, P. *Znásilnění v ČR – trestné činy a odsouzení pachatelé.*
429 Scheinost, M., Válková, H., (eds.) *Sankční politika a její uplatňování. (Teoretické a trestněpolitické aspekty reformy trestního práva v oblasti trestních sankcí IV.).*
430 Cejp, M., Blatníková, Š., Háková, L., Holas, J., Trávníčková, I. & Vlach, J. *Společenské zdroje vývoje organizovaného zločinu.*
422 Škvain, P. *Zabezpečovací detence z pohledu vybraných zahraničních právních úprav.*

2014

414 Martinková, M., Slavětínský, V. & Vlach, J. *Vybrané problémy z oblasti domácího násilí v ČR.*
415 Štěchová, M. & Večerka, K. *Systémový přístup k prevenci kriminality mládeže.*
417 Marešová, A., Cejp, M., Holas, J., Martinková, M. & Rozum, J. *Analýza trendů kriminality v roce 2013.*
418 Blatníková, Š., Faridová, P. & Zeman, P. *Násilná sexuální kriminalita – téma pro experty i veřejnost.*
419 Scheinost, M., Háková, L., Rozum, J., Tomášek, J. & Vlach, J. *Sankční politika pohledem praxe. (Teoretické a trestněpolitické aspekty reformy trestního práva v oblasti trestních sankcí II.).*

2013

403 Košťál, J. *Vybrané metody vícerozměrné statistiky.* (Vybrané metody kriminologického výzkumu – svazek 4).
404 Pojman, P. *Ruský a ukrajinský organizovaný zločin.*
405 Tomášek, J. *Self-reportové studie kriminálního chování.* (Vybrané metody kriminologického výzkumu – svazek 5).
406 Holas, J. *Politický radikalismus a mládež.*
408 Zeman, P., Diblíková, S., Slavětínský, V. & Štefunková, M. *Zkrácené formy trestního řízení – možnosti a limity.*
410 Scheinost, M., a kol. *Trestní sankce a jejich odraz v praxi, tisku a v názorech veřejnosti. (Teoretické a trestněpolitické aspekty reformy trestního práva v oblasti trestních sankcí I.).*
411 Marešová, A., Cejp, M., Holas, J., Kuchařík, K., Martinková, M. & Scheinost, M. *Analýza trendů kriminality v roce 2012.*
412 Holas, J. & Večerka, K. *Stát a občan v prevenci kriminality.*

2012

397 Cejp, M. (ed.) *Selected Results of Research Activities of ICSP in the Years 2008–2011.*
398 Marešová, A., Cejp, M., Martinková, M., Tomášek, J., Vlach, J. & Zeman, P. *Crime in the Czech Republic in 2010.*
399 Večerka, K. *Mládež o kriminalitě a etice každodennosti.*

402 Marešová, A., Biedermanová, E., Cejp, M., Holas, J., Martinková, M. & Tomášek, J. *Analýza trendů kriminality v roce 2011.*

Ediční řada Prameny:

2019

448 Heiskanen, M. & Lietonen, A. *Kriminalita a gender. Studie zaměřená na zastoupení mužů a žen v mezinárodní statistice kriminality.*

2017

442 UNODC: *Mezinárodní klasifikace trestných činů pro statistické účely.*

2016

434 Heiskanen, M., Aebi, M. E., van der Brugge, W., Jehle, J.–M. *Evidence alternativních trestů a zjišťování míry atrice. Metodologická studie komparativních dat v Evropě.*

436 *13. kongres OSN o prevenci kriminality a trestní justici. Dauhá, Katar, 12.–19. dubna 2015*

2015

420 Francis, B., Humphreys, L., Kirby, S. & Soothill, K. *Kriminální kariéra v organizovaném zločinu.*

421 Mendel, R. A. *Mládeži nepřístupno. Argumenty pro snižování počtu odnětí svobody u mladistvých.*

2014

416 Benes, M. & Astbury, B. (eds.) *Problémy trestního soudnictví: evaluace programů, prevence kriminality, strach z kriminality a recidiva – pohledem australských kriminologů.*

2013

407 United Nations Office on Drugs and Crime *Odhad nezákonných finančních toků plynoucích z obchodu s drogami a jiného nadnárodního organizovaného zločinu.*

409 United Nations Office on Drugs and Crime *Světová zpráva o obchodování s lidmi 2012.*

413 European Forum for Urban Security *Pouliční násilí v EU: Skupiny mladistvých a násilí na veřejnosti.*

2012

395 Cejp, M. (ed.) *Britské strategické dokumenty k prevenci a potírání závažné trestné činnosti.*

396 Goodey, J. & Aromaa, K. (eds.) *Trestné činy z nenávisti (příspěvky ze Stockholmského kriminologického sympozia 2006 a 2007).*

400 Marešová, A. (ed.) *Trendy kriminality ve světě a nové problémy a reakce v oblasti prevence kriminality a trestní justice.*

401 Diblíková, S. (ed.) *Rada Evropy a International Juvenile Justice Observatory k soudnictví nad mládeží.*

Plné texty všech titulů, publikovaných v edici Institutu pro kriminologii a sociální prevenci od roku 2000, jsou volně dostupné na webu IKSP www.kriminologie.cz v sekci Publikace.

Škody působené kybernetickou kriminalitou
Zpráva shrnující hlavní poznatky Pracovní skupiny k nákladům kyberkriminality

Překlad: Čeněk Novotný
Jiří Vlach
Kateřina Kudrlová

Vydavatel: Institut pro kriminologii a sociální prevenci
Nám. 14. října 12, Praha 5
Určeno: Pro odbornou veřejnost
Edice: Prameny
Design: addnoise.org
Sazba: Lukáš Pracný, sazbaknih.cz
Vydání: první – červen 2019

ISBN 978-80-7338-175-2

www.kriminologie.cz