Ing. Miroslav Čermák
Policejní akademie České republiky v Praze
student doktorského studia
Dr. Zdeněk Kovařík, CSc.
Policejní akademie České republiky v Praze
Oddělení vědy a výzkumu

Problémy determinace kybernetické bezpečnosti v prostředí České republiky – 1. část

Kybernetické útoky jsou stále sofistikovanější a nabírají na intenzitě. A nic bohužel nenasvědčuje tomu, že by se tento trend měl v dohledné době změnit. Naopak lze s ohledem na dosavadní vývoj v kyberprostoru a pokračující digitalizaci businessu očekávat, že tento trend bude nadále pokračovat.

S rostoucím počtem uživatelů, nedostatečně zabezpečených zařízení trvale připojených do internetu a na nich běžících aplikací a služeb se zvětšuje povrch útoku (attack surface). Spolu s rostoucí komplexitou systémů na jedné straně a nízkým bezpečnostním povědomím uživatelů na straně druhé, dochází ke vzniku četných zranitelností.

Tyto zranitelnosti jsou pak zneužívány útočníky k průniku do těchto systému s cílem je ovládnout a zneužít k dalším kybernetickým útokům, ať už na další informační systémy a operační technologie anebo zneužít jejich zdroje k vlastnímu obohacení či narušení jejich bezpečnosti. Tedy způsobit nedostupnost těchto systémů, pozměnit kritická data, anebo ukrást citlivé informace, která se v těchto systémech nacházejí a zpracovávají.

Bez ohledu na to, kdo za těmito útoky stojí, jaký je jeho motiv a cíl, a jakých zranitelností zneužívá, lze tyto útoky rozdělit na útoky vedené na stroje a útoky vedené na lidi, přičemž v prvním případě je zneužíváno zranitelností v návrhu, kódu a implementaci a ve druhém pak v nedostatečném bezpečnostním povědomí a nízké odolnosti vůči technikám sociálního inženýrství. Případně pak kombinaci obojího.

Stanovovat však úroveň bezpečnosti od počtu a závažnosti zranitelností, které obsahuje systém, který organizace provozuje, dost dobře nejde, neboť zranitelností je obrovské, blíže neurčené množství, a také jejich počet je velice volatilní a do značné míry i závislý na tom, kdy, kým a jak je daná zranitelnost objevena a reportována.

Co však lze identifikovat, jsou kybernetické hrozby, které se sice také vyvíjí, ale kterých je omezené množství, a které těchto zranitelností k průniku do systému zneužívají. V zásadě se dají identifikovat určité postupy, tzv. vektory útoku, které jsou pro tyto útoky společné.

V rámci probíhajícího výzkumu jsme identifikovali několik nejčastěji používaných vektorů útoku a rovněž i následků těchto útoků, které jsou popsány v bezpečnostních reportech firem nabízejících bezpečnostní řešení a dále pak ve spolupráci s bezpečnostními experty navrhli základní sadu bezpečnostních opatření, která by měla organizaci před těmito útoky ochránit.

Zbytkové riziko by pak mělo být pokryto kybernetickým pojištěním. K tomu, aby však mohlo být navrhnuto takové pojištění, které by bylo pro obě strany výhodné, bylo nutné ověřit, jakým kybernetickým útokům a jak často organizace čelí, jaký je použit vektor útoku a jaké jim vznikají škody.

Vzhledem k tomu, že drtivá většina bezpečnostních reportů a výzkumů je zahraniční provenience, a tudíž není zřejmé, jaká je skutečná situace v kyberprostoru v ČR, tedy jakým útokům organizace v ČR čelí, obrátili jsme se formou dotazníkového šetření na manažery informační bezpečnosti v organizacích v ČR a požádali je o zodpovězené otázek týkajících se zavedení vybrané sady bezpečnostních opatření, četnosti výskytu jednotlivých vektorů útoku (attack vector) a dopadů těchto útoků.

V tomto článku se věnujeme vztahu mezi velikostí a sektorem organizace na jedné straně a zavedenými bezpečnostními opatřeními, vektory útoku, incidenty a obavami na straně druhé.

Základní výzkumný předpoklad

V rámci analýzy dat z výzkumu byl ověřován následující výzkumný předpoklad:

VP_0: Na odpovědi expertů výběrového souboru vztahující se k problematice kybernetické bezpečnosti zkoumaných organizací nebude mít akceptovatelný věcně významný vliv sektor ani velikost organizace, ve kterých tito experti působí (koeficienty Tau nebo $\beta \geq 0{,}01$; Cohenovo $w \geq 0{,}1$).

Složení výběrového souboru

Respondenti byli vybráni z řad expertů, kteří se zaobírají problematikou kybernetické bezpečnosti v rámci své organizace. Základní složení výběrového souboru obsahují následující tabulky.

V Tabulce č. 1 je zachycen podíl soukromého a veřejného sektoru na celkovém počtu respondentů. V rámci tohoto příspěvku se jedná o proměnnou označenou jako ID01.

Tabulka č. 1

V jakém působíte sektoru

		Četnost	Procenta
Platná	Soukromý	64	68,8
	Veřejný	29	31,2
	Celkem	93	100,0

V Tabulce č. 2 je zachycen podíl organizací o různé velikosti na celkovém počtu respondentů. V rámci tohoto příspěvku se jedná o proměnnou označenou jako ID03.

Tabulka č. 2

Jak velká je vaše organizace

		Četnost	Procenta
Platná	Mikropodnik do 10 osob	14	15,1
	Malý podnik od 10 do 50 osob	13	14,0
	Střední podnik od 50 do 250 osob	19	20,4
	Velký podnik nad 250 osob	47	50,5
	Celkem	93	100,0

Otázky pokládané bezpečnostním expertům v rámci tohoto výzkumu se týkaly zavedení vybrané sady bezpečnostních opatření, vektorů útoku, incidentů a obav. Celkem se jednalo o 54 uzavřených dichotomických a polychotomických otázek, které jsou kódovány jako P, za kterým pak následuje pořadové číslo otázky. V rámci analýzy dílčích závislostí pak byl zkoumán vztah mezi jednotlivými otázkami P01 až P54 a identifikátory ID01 a ID03. V Tabulce č. 3. jsou uvedeny jen ty otázky, kde byl nějaký vztah nalezen.

Tabulka č. 3

P	Otázka
01	Šifrujete data na disku vašeho koncového zařízení?
08	Můžete na svém koncovém zařízení spustit jakýkoliv program nebo skript?
11	Zaznamenali jste skenování, inventarizaci, enumeraci ve vašich systémech?
18	Byl někomu z vašich zaměstnanců doručen spear phishing e-mail?
19	Volal do vaší firmy někdo, kdo se vydával za někoho jiného a snažil se ze zaměstnanců vytáhnout informace?
23	Došlo u vás k výpadku proudu?
33	Došlo k zašifrování některých vašich dat ransomwarem?
50	Obáváte se sabotáže ze strany zaměstnance?
51	Obáváte se očerňující kampaně na internetu?

Základní metodologické hledisko pro analýzu dat z nenáhodných výběrů

Výběrový soubor byl pořízen na základě dostupnosti. Proto nelze závěry zobecňovat na základní soubor; budou mít platnost pouze pro daný výběrový soubor. Z toho vyplývá, že statistická významnost (p-value[1]) pozbývá v tomto případě svůj hlavní význam, lze podle ní jen odhadovat dostatečnost rozsahu výběrového souboru.

[1] Hladina významnosti (p-value) odráží nejen sílu vztahu (míru asociace), ale je v přísné návaznosti na velikost výběrového souboru. Někdy odráží i vliv jiných parametrů. Proto je v rámci náhodného výběru možné mít vztah mezi proměnnými, který vyjadřuje silnou asociaci, ale není statisticky významný. To proto, že rozsah je velmi malý. Na druhou stranu mohou existovat vztahy, které zobrazují extrémně slabou asociaci, ale jsou statisticky velmi významné.

Z předchozího bodu odstavce také vyplývá, že nelze pro ověřování vztahů mezi proměnnými použít statistické testování hypotéz, právě s ohledem na neexistenci náhodného výběru. Pro ověřování vztahů mezi proměnným bude tudíž využito pojmu „**ověřování výzkumného předpokladu**“ (tento pojem není omezen podmínkami induktivní statistiky).

Důvodem, proč jsou v rámci empirického výzkumu jeho výstupy posuzovány užitím věcné významnosti, je kladení důrazu na kritické posouzení a praktické využití analýzy dat. Soukup[1] uvádí, že věcná významnost výsledku znamená, že naměřený rozdíl či zjištěná souvislost je důležitá pro vědecké poznání či praktické účely.

Věcná významnost umožňuje rozhodnout, zda o výsledku má smysl polemizovat a zdá má praktické důsledky, a to i pro vědecké účely. Ke zjištění, zda je výsledek věcně významný a v jakém rozsahu, se využívají ukazatele, tzv. míry věcné významnosti („effect size“).

Stanovení kritérií a ukazatelů pro ověřování výzkumných předpokladů

1) Jako **základní kritérium** pro ověřování výzkumných předpokladů u kategorizovaných proměnných lze zvolit **věcnou významnost reálného rozdílu na úrovni 10 %**[2] mezi adekvátními řádkovými relativními četnostmi v rámci porovnávaných uzlů u klasifikačních stromů (stejné řádky u koncových uzlů klasifikačního stromu, které mají největší heuristický význam).

2) Jako **pomocný ukazatel** zjištěných věcně významných rozdílů bude použito pro **nominální proměnné** asymetrické **Goodmanovo a Kruskalovo tau**, které má přímou procentuální interpretaci. Goodmanovo a Kruskalovo tau vyjadřuje podíl vysvětleného „nomvar“ závislé nominální proměnné ve třídách nominální proměnné nezávislé.

3) Za situace asymetrického vlivu **nominální proměnné na proměnnou ordinální** bude použit Řehákův koeficient asociace β (ordinální regresní závislosti).[3] Asymetrický koeficient β vyjadřuje podíl vysvětleného rozptylu ordinální proměnné B ve třídách nominální proměnné A. Ordinální statistická závislost se projevuje ve změně tvaru podmíněných rozložení nebo posunutí na škále znaku. Pokud 95% interval spolehlivosti u koeficientu β obsahuje nulovou hodnotu, znamená to, že rozsah výběrového souboru by měl být větší. Měření věcně významného vlivu zabezpečuje symetrický index Cohenovo w.[4]

Vzhledem k tomu, že asymetrický koeficient tau i koeficient β mají přímou, procentuální interpretaci, lze analogicky přijmout pro jejich interpretaci konvenčně uznávané hodnoty koeficientu ω^2 (0,01 – malý efekt; 0,059 – střední efekt; 0,138 –

[1] SOUKUP, Petr. Substantive significance and it´s measures. *Data and Research – SDA Info* [online]. 2013, 127(2), 125- [cit. 2018-01-30]. DOI: 10.13060/23362391.2013.127.2.41. ISSN 23362391. Dostupné z: http://dav.soc.cas.cz/issue/19-data-a-vyzkum-2-2013/111.

[2] Dosavadní zkušenosti z analýzy dat ukazují, že zjištěný minimální 10% rozdíl v řádkových relativních četnostech je zpravidla doprovázen min. velikostí Cohenova indexu „w“ na úrovni $w \geq 0{,}10$.

[3] Srov. ŘEHÁK, Jan a Blanka ŘEHÁKOVÁ. *Analýza kategorizovaných dat v sociologii*. Praha: Academia, 1986, s. 250.

[4] V případě příznivějších hodnot asymetrických koeficientů asociace (tau, β) je upřednostníme před hodnotami symetrického Cohenova indexu w.

velký efekt).[1] Při porovnání hodnot asymetrických koeficientů asociace respektujeme stanovisko de Vause. Dle něj obecně platí, jestliže Goodman a Kruskalovo tau je vyšší než koeficient β, pak to pravděpodobně signalizuje existenci nominálního statistického vztahu, nikoli ordinálního.[2]

V tabulce č. 1 je uveden přehled používaných koeficientů a indexů věcné významnosti. V kontingenční tabulce je uveden index w s vymezením věcně významného vlivu (0,1 – malý věcně významný vliv, 0,3 – střední věcně významný vliv, 0,5 – velký věcně významný vliv).[3]

Tabulka č. 1

Test	Relevant effect size	Effect size classes		
		Small	Medium	Large
Comparison of independent means	d, Δ, Hedges' g	.20	.50	.80
Comparison of two correlations	q	.10	.30	.50
Difference between proportions	Cohen's g	.05	.15	.25
Correlation	r	.10	.30	.50
	r^2	.01	.09	.25
Crosstabulation	w, φ, V, C	.10	.30	.50
ANOVA	f	.10	.25	.40
	η^2	.01	.06	.14
Multiple regression	R^2	.02	.13	.26
	f^2	.02	.15	.35

Postup ověřování výzkumných předpokladů při analýze dat a výpočtu vymezených koeficientů a indexů

Pro analýzu závislostí mezi vybranými kategorizovanými proměnnými byl použit program IBM SPSS Modeler V18.2.1, konkrétně jeho modul pro vytvoření klasifikačního stromu prostřednictvím algoritmu CHAID.

Pro výpočet asymetrického koeficientu Goodman a Kruskal tau byl použit program IBM SPSS Statistics V26. Pro výpočet asymetrického koeficientu β byla využita utilita nadstandardně vytvořená pro systém SPSS. Cohenův index w byl zjištěn za pomoci programu NCSS PASS.

Analýza dílčích závislostí

Analýza odhalila určité rozdíly a závislosti mezi některými proměnnými. Ty jsou okomentovány níže.

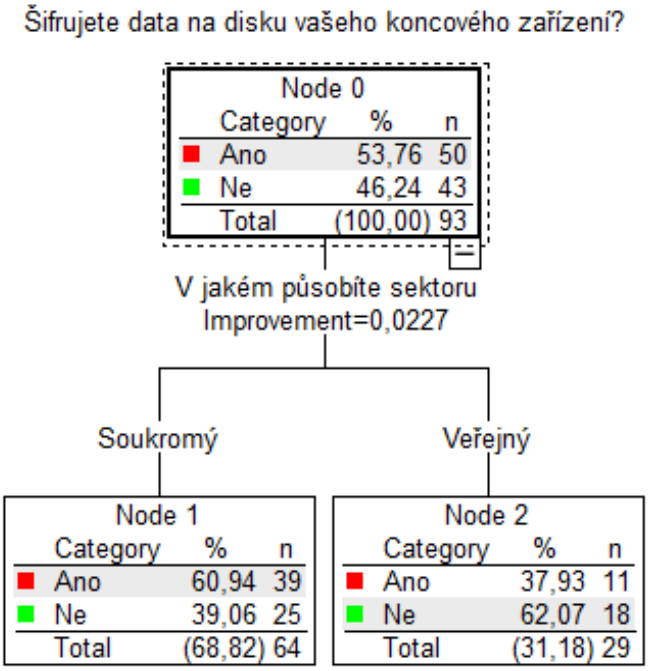
[1] Srov. KIRK, Roger E. *Statistics: An Introduction*. 5. vyd. Belmont: Thomson Wadsworth, 2007, s. 475.
[2] Srov. DE VAUS, David A. *Surveys in Social Research*. 5. vyd. Crows Nest: Allen & Unwin, 2002, s. 260-262.
[3] ELLIS, Paul D. The Essential Guide to Effect Size. Statistical Power, Meta-Analysis, and the interpretation of Research Results. New York: Cambridge University Press 2010, p. 41.

Uvedené klasifikační stromy obsahují absolutní a relativní četnosti porovnávaných odpovědí daných koncových uzlů s orientačním uvedením hodnot testů nezávislosti chí-kvadrát, statistické významnosti a stupňů volnosti. Pod klasifikačními stromy jsou uvedeny hodnoty adekvátních koeficientů a indexů asociace a věcné významnosti.

Dále pak proběhla explanační analýza ve spolupráci s bezpečnostními experty, kdy byly identifikovány možné příčiny tohoto stavu, které jsou uvedeny vždy pod příslušnými stromy.

Vliv ID01 - V jakém působíte sektoru (P01, P19, P23, P51)

Vliv ID01 – P01



Goodman a Kruskalovo tau = 0,046 (větší než malá věcně významná asociace)
Symetrický Cohenův index w = 0,213 (větší než malý věcně významný efekt)

Šifrování dat lze zahrnout mezi základní bezpečnostní opatření technické povahy, které poskytuje zajištění důvěrnosti dat v případě, že dojde ke zcizení média, na kterém se nacházejí citlivá data anebo celého koncového zařízení, na kterém jsou data rovněž uložena a zpracovávána. Přesto téměř polovina respondentů (46,24 %) svá data nešifruje, zatímco více jak polovina svá data šifruje (53,76 %).

Netřeba dodávat, že neoprávněná osoba, která k datům ať už na přenosném médiu nebo na samotném zařízení získá přístup, není schopna se bez znalosti hesla k datům dostat. Skutečnost, že organizace působící v soukromém sektoru ve výrazně větší míře šifrují data na svých koncových zařízeních (60,94 %), než organizace působící ve státním sektoru (37,93 %) si lze vysvětlit tak, že:

- jejich vlastníci a manažeři jsou si více vědomi hodnoty svých informací, které obzvláště ve vysoce konkurenčním a turbulentně se měnícím prostředí jsou předmětem nejrůznějších kybernetických útoků, konkurenčního zpravodajství a průmyslové špionáže a mohou představovat značnou konkurenční výhodu

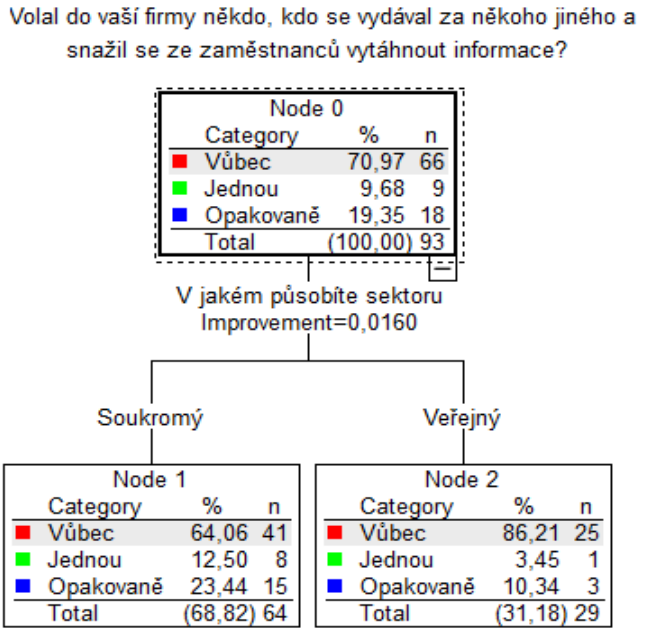
a i jejich pouhý únik může značně poškodit dobré jméno organizace a v konečném důsledku vést i k ukončení její činnosti na trhu, což je pro ně vyšší riziko než pouhá pokuta od ÚOOÚ;

- organizace působící ve statním sektoru, a mající zpravidla i monopol na poskytování určité činnosti nemusí příliš ztrátu svého dobrého jména řešit, neboť mohou maximálně dostat pokutu od ÚOOÚ, ale ve své činnosti budou vzhledem ke svému monopolnímu postavení nadále pokračovat;
- většina zaměstnanců působících ve státním sektoru pracuje na nepřenosných zařízeních, desktopech, umístěných v kancelářích, kam za ní sice chodí veřejnost, ale kde nemůže dojít a ani nedochází k jejich krádeži a pokud už jsou zaměstnanci vybaveni notebooky, tak se s nimi zpravidla pohybují jen v prostorách svého zaměstnavatele;
- zaměstnanci působící v soukromých společnostech pracují v open space, kavárnách a na home office, kde buď dochází k většímu pohybu velkého množství osob, včetně externistů, zaměstnanci se mezi sebou neznají anebo pracují z domova, kde není zajištěna stejná úroveň fyzické bezpečnosti, a kde je riziko krádeže výrazně vyšší;
- zaměstnanci působící v soukromém sektoru za svými zákazníky více cestují, více využívají možnosti home office a zdá se, že tento trend bude dál pokračovat,[1] a bude zde i vyšší riziko, že své přenosné zařízení ztratí anebo jim bude ukradeno;
- v neposlední řadě šifrování něco stojí, a ne všechny organizace disponují zařízeními a operačními systémy, která transparentní šifrování podporují a mají vyřešenu správu klíčů (key management).

Z rozhovoru s manažery informační bezpečnosti dále vyplynulo, že k šifrování koncových zařízení přistoupili neprodleně poté, co řešili až několik případů ročně, kdy došlo ke ztrátě a krádeži notebooků z šatních skříní, v restauracích, zaparkovaných aut apod. a nechtěli riskovat, že by se případný útočník mohl dostat k citlivým datům na nich uložených. A v mnoha případech nešlo ani tak o to, že by je zpřístupnění dat mohlo přímo ohrozit, jako spíše o poškození dobrého jména organizace v důsledku možné medializace takového případu.

[1] HAMROZI, Petr. V IT byl homeoffice běžný, po koronaviru dál poroste [online]. [vid. 8. červen 2020]. Získáno z: https://www.nejbusiness.cz/zpravy/2020-05-06-v-it-byl-homeoffice-bezny-po-koronaviru-dal-poroste

Vliv ID01 – P19



Volal do vaší firmy někdo, kdo se vydával za někoho jiného a snažil se ze zaměstnanců vytáhnout informace?	V jakém působíte sektoru				
	Soukromý	Veřejný	celkem	medián	dorvar
Vůbec	-	+	66	1,305	,471
Jednou	o	o	9	1,063	,198
Opakovaně	o	o	18	1,100	,278
celkem	64	29	93	1,227	,429

Hodnota koeficientu beta je 0,052 s 95 % intervalem spolehlivosti (-0,025; 0,129) (téměř střední věcně významná asociace)
Symetrický Cohenův index w = 0,228 (větší než malý věcně významný efekt)

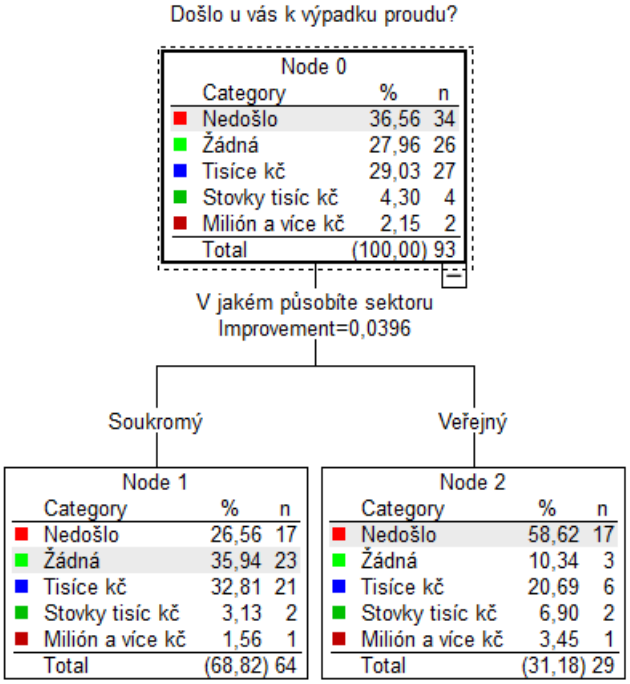
Hodnota koeficientu beta je 0,052 s 95 % intervalem spolehlivosti (-0,025; 0,129)
Cohenův index w = 0,228 (více než malý věcně významný efekt)

Vishing neboli phishing po telefonu patří mezi nejjednodušší techniku sociálního inženýrství, kdy se útočník vydává za někoho jiného a snaží se tak získat citlivé informace. Opakovaně se s ní setkala přibližně pětina organizací (19,35 %) a alespoň jednou pak necelá desetina (9,68 %). Skutečnost, že většina oslovených organizací (70,97 %) se s ní nesetkala, by nasvědčovalo tomu, že je tato technika využívána výhradně v rámci cílených útoků na konkrétní organizace a není na rozdíl od phishingu aplikována plošně, nejspíš proto, že je dražší a vyžaduje větší přípravu. Skutečnost, že se s touto technikou ve větší míře opakovaně setkávají spíše zaměstnanci soukromých společností (23,44 %) než zaměstnanci ve veřejném sektoru (10,34 %), je možné vysvětlit tak, že:

- v drtivé většině soukromých organizací lze zaznamenat zahraniční účast a tudíž je běžné, že zaměstnanci těchto organizací jsou jazykově lépe vybaveni a jsou zvyklí, že jim běžně volají kolegové ze zahraničních poboček s nejrůznějšími dotazy.
- v soukromých organizacích je soustředěno know-how, a je obtížnější zaměstnance těchto organizací přesvědčit ke spolupráci, což může být dáno např. i vyšším finančním ohodnocením.

- Drtivá většina zaměstnanců působících ve veřejném sektoru slouží občanům ČR a jako úřední jazyk používají češtinu, takže tak často do styku se zahraničními občany nepřijdou a osoba hovořící anglicky by upoutala jejich pozornost a svého cíle by nedosáhla.

Vliv ID01 – P23



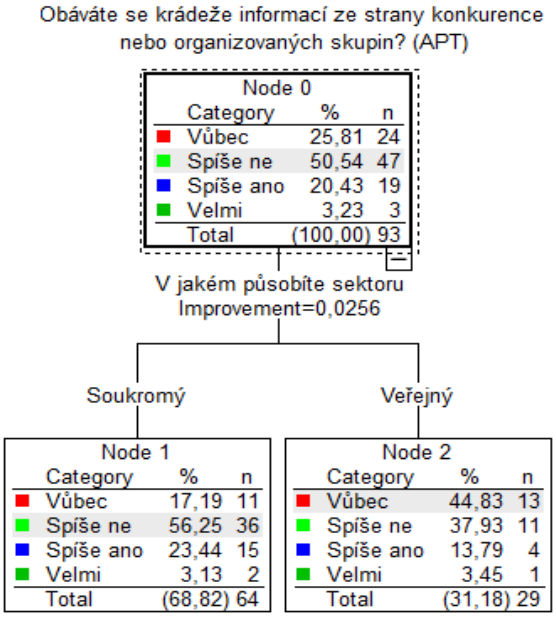
Došlo u vás k výpadku proudu?	V jakém působíte sektoru				
	Soukromý	Veřejný	celkem	medián	dorvar
Nedošlo	--	++	34	1,500	,500
Žádná	+	-	26	1,065	,204
Tisíce kč	o	o	27	1,143	,346
Stovky tisíc kč	o	o	4	1,500	,500
Milión a více kč	o	o	2	1,500	,500
celkem	64	29	93	1,227	,429

Hodnota koeficientu beta je 0,132 s 95 % intervalem spolehlivosti (-0,001; 0,266) (velká věcně významná asociace)
Symetrický Cohenův index w = 0,363 (střední věcně významný efekt)

- Na dodávce proudu je většina ekonomických subjektů závislá a jeho výpadek jim může způsobit s ohledem na délku jeho trvání nemalé problémy v podobě finanční ztráty v různé výši.
- Zatímco více jak čtvrtina (25,56 %) organizací působících v soukromém sektoru se s tímto incidentem nesetkala, tak organizací působících ve veřejném sektoru se s tímto incidentem nesetkala více jak polovina (58,62 %). Rozdíl mezi organizacemi působícími v soukromém a veřejném sektoru se pak projevuje i ve výši škod, zatímco v soukromém sektoru utrpěla škodu ve výši několika tisíc korun téměř třetina organizací (32, 81 %), tak ve veřejném sektoru to byla jen pětina (20,69 %).

Ovšem na druhou stranu zase mnohem méně organizací ze soukromého sektoru utrpělo škodu ve výši stovek tisíc korun anebo dokonce přesahujících milión korun.

Vliv ID01 – P51



Obáváte se krádeže informací ze strany konkurence nebo organizovaných skupin? (APT)	V jakém působíte sektoru				
	Soukromý	Veřejný	celkem	medián	dorvar
Vůbec	--	++	24	1,577	,497
Spíše ne	o	o	47	1,153	,359
Spíše ano	o	o	19	1,133	,332
Velmi	o	o	3	1,250	,444
celkem	64	29	93	1,227	,429

Hodnota koeficientu beta je 0,088 s 95 % intervalem spolehlivosti (-0,036; 0,211) (střední věcně významná asociace)
Symetrický Cohenův index w = 0,296 (střední věcně významný efekt)

V současné době, která je nazývána jako informační, se s informacemi obchoduje jako s jakoukoliv jinou komoditou,[1] neboť ten, kdo má k dispozici informace a dokáže jich využít, získává na turbulentně se měnícím trhu nezanedbatelnou konkurenční výhodu. Nelze se tak divit, že předmětem cílených kybernetických útoků vedených na informační systémy a zaměstnance určitých organizací jsou právě informace.

Skutečnost, že více jak čtvrtina (25,81 %) respondentů se těchto útoků neobává vůbec a spíše ne pak více jak polovina (50,54 %) nasvědčuje tomu, že jsou tyto útoky ze strany respondentů vnímány stále jako něco, co se jich přímo netýká. Určitou obavu

[1] ANDREW PREATER. Information as a commodity – at #radliblon. *Andrew Preater* [online]. 3. červen 2014 [vid. 8. červen 2020]. Získáno z: https://www.preater.com/2014/06/03/information-as-a-commodity/

vyjádřila přibližně pětina respondentů (20,43 %) a velmi se obává jen pouhých pár procent (3,23 %) respondentů.

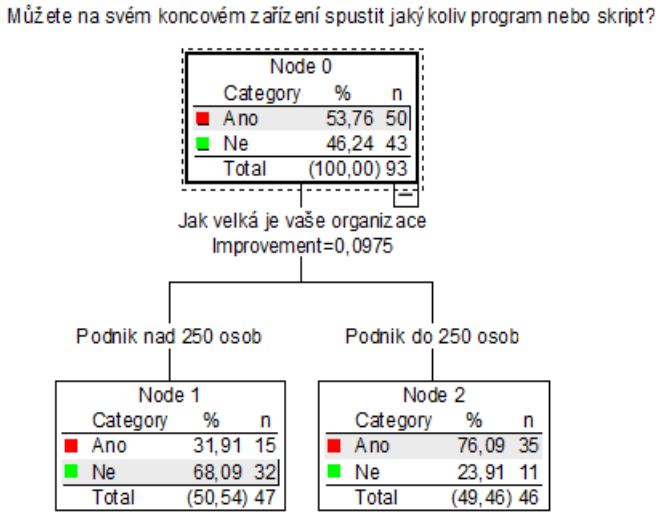
Určité rozdíly pak lze zaznamenat mezi tím, jak tuto hrozbu vnímají respondenti v soukromém a veřejném sektoru. Jen necelá pětina respondentů v soukromém sektoru se této hrozby neobává vůbec (17,19 %) a spíše se neobává více jak polovina (56,25 %), ve veřejném sektoru se neobává podstatně více respondentů, téměř polovina (44,83 %), ale spíše se neobává jen více jak třetina (37,93 %).

Vyšší obava respondentů působících v soukromém sektoru se dá vysvětlit tím, že je na ně buď vedeno více útoků anebo jsou více závislé na hospodářských výsledcích organizace, ve které působí, případně se může jednat i o kombinaci obou těchto faktorů. Opomenout také nelze ani působení médií, i když v tomto případě lze vzhledem k počtu medializovaných případů o síle tohoto faktoru pochybovat. V dalším výzkumu by však bylo vhodné se zaměřit na to, co přesně ovlivňuje obavy respondentů, protože z rozhovoru s nimi vyplynulo, že od těchto jejich obav se v zásadě odvíjí obsah jejich strategie informační bezpečnosti na další rok.

Vliv ID03 - Jak velká je vaše organizace (P08, P11, P18, P33, P50)

Vliv ID03 na P08

Otázka ohledně možnosti spustit jakýkoliv program nebo skript je klíčová, protože toto opatření patří mezi nejúčinnější, pokud jde o kompromitaci koncového zařízení prostřednictvím škodlivého kódu. Více jak polovina respondentů (53,76 %) se vyjádřila, že na svém zařízení může spustit jakýkoliv program nebo skript a necelá polovina (46,24 %), že nikoliv.

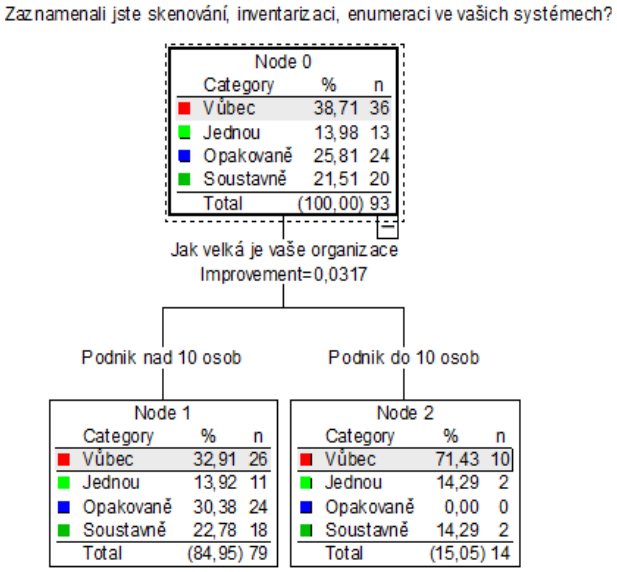


Goodman a Kruskalovo tau = 0,196 (velká věcně významná asociace)
Symetrický Cohenův index w = 0,443 (téměř velký věcně významný efekt)

Dále se se ukázalo, že je zde značný rozdíl mezi tím, jak k této problematice na jedné straně přistupují velké organizace, kde jen přibližně třetina (31,91 %) může na svém zařízení spustit libovolný kód a na straně druhé mikropodniky, malé a střední podniky, kde jsou to více jako tři čtvrtiny (76,09 %), kterým to bezpečnostní politika nezakazuje. Je možné, že příčinou tohoto rozporu jsou následující skutečnosti:

- velké společnosti si uvědomují, že možnost spouštět na koncovém zařízení uživatele jakýkoliv program sice zvyšuje uživatelský komfort, ale na druhou stranu zde hrozí riziko používání SW v rozporu s licenčním ujednáním, kdy spousta SW nesmí být používána pro komerční účely;
- velké společnosti si uvědomují, že stejně jako může být spuštěn jakýkoliv skript nebo aplikace stažená z internetu, zaslaná e-mailem anebo donesená na přenositelném médiu, tak stejně tak může být spuštěn i škodlivý kód doručený obdobným způsobem a spuštěn pod profilem a s právy aktuálně přihlášeného uživatele;
- náklady na zabezpečení koncového zařízení ve smyslu blokování neschválených aplikací, což je možné prostřednictvím funkcí operačního systému anebo bezpečnostních aplikací třetích stran, kdy lze vhodná pravidla nastavit tak, aby se daly spustit jen nainstalované aplikace a nové aplikace uživatel nainstalovat nemohl a nemohl ani spouštět neschválené skripty spouštěné pomocí schválených příkazových interpretů;
- spoléhají na zabezpečení na úrovni antimalware řešení, které by měly detekovat škodlivý kód.

Vliv ID03 na P11



Zaznamenali jste skenování, inventarizaci, enumeraci ve vašich systémech?	Jak velká je vaše organizace				
	Podnik do 10 osob	Podnik nad 10 osob	celkem	medián	dorvar
Vůbec	++	--	36	1,808	,401
Jednou	o	o	13	1,909	,260
Opakovaně	-	+	24	2,000	,000
Soustavně	o	o	20	1,944	,180
celkem	14	79	93	1,911	,256

Hodnota koeficientu beta je 0,099 s 95 % intervalem spolehlivosti (0,006; 0,192) (více než střední věcně významná asociace)
Symetrický Cohenův index w = 0,396 (více než střední věcně významný efekt)

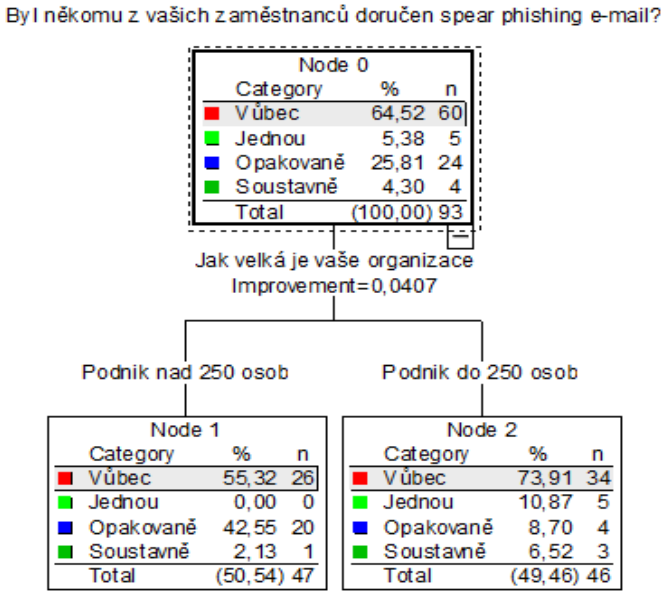
Otázka týkající se skenování, inventarizace a enumerace v systémech organizace, resp. zda organizace tuto skutečnost zaznamenala, odhalila, že téměř dvě pětiny (38,71 %) organizací tuto skutečnost nezaznamenaly, více jako pětina (13,98 %) ji zaznamenala během roku jednou a čtvrtina (25,81 %) eviduje opakované skenování svých systémů a pětina (21,51 %) pak detekuje tuto aktivitu dokonce soustavně.

Je otázka, zda ti, co skenování, inventarizaci ani enumeraci ve svých systémech nezaznamenali, ji nezaznamenali proto, že se o to nikdo nepokoušel anebo proto, že nemají prostředky, kterými by to zjistili. Vzhledem k tomu, že k plošným skenům celého internetu dochází spolu se zveřejněním každé kritické zranitelnosti v hojně používaných produktech, kloníme se spíš k druhé hypotéze.

Dále jsme zaznamenali, že mezi podniky nad 10 osob a do 10 osob jsou značné rozdíly. Zatímco v první skupině je jen necelá třetina organizací (32,91 %), které sken nezaznamenaly, tak ve druhé skupině jsou to téměř tři čtvrtiny (71,43 %). Příčina tohoto stavu může spočívat především v tom, že:

- prvně jmenovaní si uvědomují, že skenování, inventarizace a enumerace jsou prvním krokem, který útočník realizuje v rámci plošně i cíleně vedených kybernetických útoků, a tudíž zavedli taková bezpečnostní opatření, pomocí kterých jsou schopni tuto první fázi útoku detekovat;
- druzí jmenovaní si tuto skutečnost nepřipouští, nemají zdroje, a to ani finanční ani lidské na to, aby mohly odpovídající bezpečnostní řešení realizovat. A rovněž z rozhovorů s vlastníky mikropodniků a ředitelů malých firem vyplynulo, že si skutečnost, že by na ně mohly být vedeny cílené útoky, nepřipouští a stejně tak si nepřipouští, že by se jejich organizace mohly stát obětí tzv. plošného útoku.

Vliv ID03 na P18



Byl někomu z vašich zaměstnanců doručen spear phishing e-mail?	Jak velká je vaše organizace				
	Podnik do 250 osob	Podnik nad 250 osob	celkem	medián	dorvar
Vůbec	0	0	60	1,382	,491
Jednou	+	-	5	1,000	,000
Opakovaně	---	+++	24	1,900	,278
Soustavně	0	0	4	1,167	,375
celkem	46	47	93	1,511	,500

Hodnota koeficientu beta je 0,191 s 95 % intervalem spolehlivosti (0,061; 0,32) (velká věcně významná asociace)
Symetrický Cohenův index w = 0,437 (téměř velký věcně významný efekt)

Spear phishing je nejčastější modus operandi používaný v rámci cílených útoků na konkrétní organizace, kdy jsou zneužívány techniky sociálního inženýrství k oslovování čelních představitelů organizace, ale i řadových zaměstnanců e-mailem, ve kterém jsou tito vyzýváni ke kliknutí na odkaz v e-mailu anebo přílohy v něm uvedené. Kvalita těchto e-mailů se může podstatně lišit, v rámci vyšetřování bezpečnostních incidentů tohoto typu v posledních letech byly zaznamenány kampaně, kde se obětí stali i bezpečnostní experti a specialisté, což vypovídá o vysoké nebezpečnosti a kvalitě těchto útoků, které byly v souladu s metodikou hodnocení míry nebezpečnosti phishingových útoků[1] hodnoceny jako kritické.

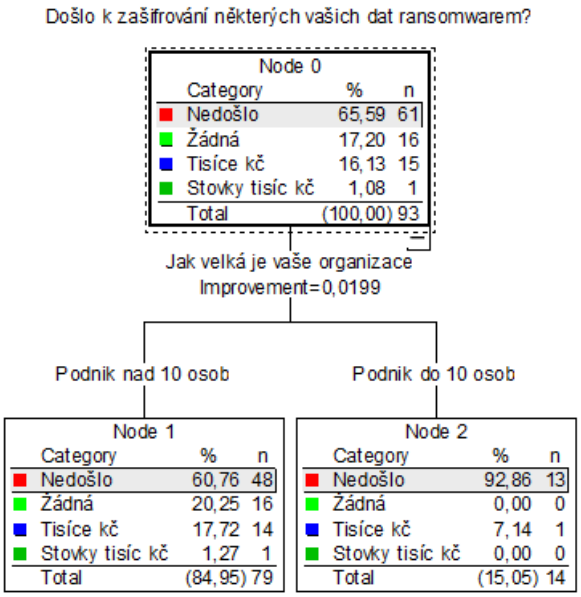
Více jak dvě třetiny respondentů (64,52 %) se s touto technikou nesetkalo vůbec, a čtvrtina (25,81 %) se s ní pak setkává opakovaně. Zde nelze argumentovat tím, že by se organizace s tímto typem útoku nesetkala proto, že by byl předmětný e-mail zastaven v perimetru dříve, než by byl doručen, protože pak by se nejednalo s největší pravděpodobností o spear phishing, ale obyčejný phishing. Daleko spíš lze předpokládat, že tyto cílené útoky jsou vedeny jen na některé organizace a pokud má útočník zájem do dané organizace proniknout, tak se o to pokouší i opakovaně.

Objevují se zde rozdíly mezi organizacemi nad 250 osob a do 250 osob. Jestli se v první skupině více jak polovina (55,32 %) respondentů s tímto útokem nesetkala vůbec, tak ve druhé skupině to byly dokonce téměř tři čtvrtiny (73,91 %) respondentů. Bez povšimnutí také nemůžeme nechat skutečnost, že v podniku nad 250 osob se s tímto typem útoku respondenti setkávají opakovaně (42,55 %), zatímco v podniku do 250 osob se opakovaně s tímto útokem setkává výrazně méně respondentů (8,7 %).

To si lze vysvětlit tak, že v menší organizaci se informace o tom, že zde proběhl nějaký spear phishing šíří mnohem rychleji a je možné všechny zaměstnance lépe seznámit s tím, co se stalo a útočník si proto s opakováním útoku dává na čas. Další důvod pak může být ten, že je zde omezený počet zaměstnanců, na které lze cílit.

[1] HOAX | Metodika hodnocení míry nebezpečnosti [online]. [vid. 8. červen 2020]. Získáno z: https://hoax.cz/cze/metodika-hodnoceni-miry-nebezpecnosti/

Vliv ID03 na P33



Došlo k zašifrování některých vašich dat ransomwarem?	Jak velká je vaše organizace				
	Podnik do 10 osob	Podnik nad 10 osob	celkem	medián	dorvar
Nedošlo	+	-	61	1,865	,335
Žádná	o	o	16	2,000	,000
Tisíce kč	o	o	15	1,964	,124
Stovky tisíc kč	o	o	1	2,000	,000
celkem	14	79	93	1,911	,256

Hodnota koeficientu beta je 0,061 s 95 % intervalem spolehlivosti (0,001; 0,119) (střední věcně významná asociace)
Symetrický Cohenův index w = 0,248 (téměř střední věcně významný efekt)

Otázka týkající se zašifrování data ransomwarem odhalila, že navzdory tvrzení médií, že ransomware představuje největší hrozbu, tak u téměř dvou třetin (65,59 %) organizací k žádnému spuštění ransomware nedošlo, u necelé pětiny (17,2 %) nedošlo k žádné škodě a u téměř stejného počtu organizací (16,13 %) došlo jen ke škodě v řádu tisíců a u pouhého procenta (1,08 %) se škoda pohybovala ve výši stovek tisíc korun.

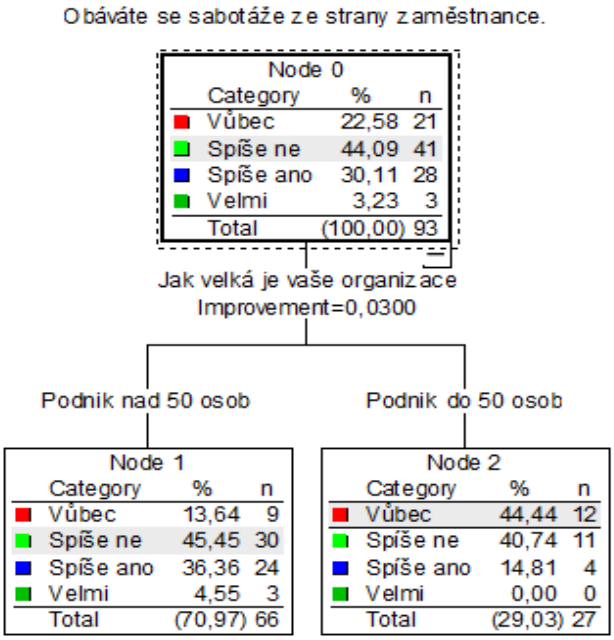
To může znamenat, že tyto útoky nejsou až tak časté, jsou detekovány včas a organizace mají zavedeny efektivní postupy. Ukázalo se také, že výše škody do určité míry závisí na velikosti organizace, neboť organizace nad deset zaměstnanců reportují škodu v řádech tisíců (17,72 %) oproti (7,14 %) organizací do deseti zaměstnanců, což dává smysl, protože:

- cena za výpalné byla fixní, uvedená v bitcoinech a v možnostech organizace ji zaplatit;
- čím větší je organizace, tím více má zaměstnanců a výpočetní techniky a tím více zařízení může být v případě úspěšného napadení zašifrováno, a tedy i dat na nich;

- to v konečném výsledku vede ke zvýšení nákladů na obnovu dat, která se odvíjí od množství zašifrovaných dat a dostupnosti záloh, přičemž zašifrovány mohou být i poslední zálohy;
- v okamžiku, kdy nejsou k dispozici zálohy, ze kterých by se dala data obnovit, tak se tato data musí pořídit a zpracovat znovu.

Nemusí tomu tak však být i nadále, protože z rozhovoru s některými bezpečnostními experty vyplynulo, že v tomto roce, se i u nás začínají objevovat útoky, kdy útočník v okamžiku, kdy zjistí, kdo se stal obětí, tak zvyšuje cenu výkupného a snaží se smlouvat[1] a je možné, že i výše výpalného se může do budoucna odvíjet od postavení daného subjektu na trhu.

Vliv ID03 na P50



Obáváte se sabotáže ze strany zaměstnance.	Jak velká je vaše organizace				
	Podnik do 50 osob	Podnik nad 50 osob	celkem	medián	dorvar
Vůbec	++	--	21	1,375	,490
Spíše ne	o	o	41	1,817	,393
Spíše ano	-	+	28	1,917	,245
Velmi	o	o	3	2,000	,000
celkem	27	66	93	1,795	,412

Hodnota koeficientu beta je 0,133 s 95 % intervalem spolehlivosti (-0,008; 0,273) (téměř velká věcně významná asociace)
Symetrický Cohenův index w = 0,364 (více než střední věcně významný efekt)

[1] HALLER, Martin. Jak vypadá vyjednávání o výkupném u ransomware. *Martin Haller* [online]. 11. květen 2020 [vid. 8. červen 2020]. Získáno z: https://martinhaller.cz/ransomware/jak-vypada-vyjednavani-o-vykupnem-u-ransomware/

Obava týkající se sabotáže ze strany vlastního zaměstnance je větší ve velkých a střednících organizacích než v malých podnicích a mikropodnicích. To může být dáno mimo jiné tím, že:

- zaměstnanci mikropodniků a malých podniků mají větší pocit sounáležitosti s podnikem, jsou často rodinnými příslušníky, podílníky a jsou na existenci podniku životně závislí, mezi sebou se lépe znají a důvěřují si a tudíž se sabotáže tak neobávají.
- velké a střední podniky často uvádí vyšší míru fluktuace, nižší loajalitu zaměstnanců, a rovněž na tuto otázku odpovídá bezpečnostní manažer, který zpravidla jednotlivé zaměstnance nezná, a tak na ně nahlíží s jistou dávkou nedůvěry.

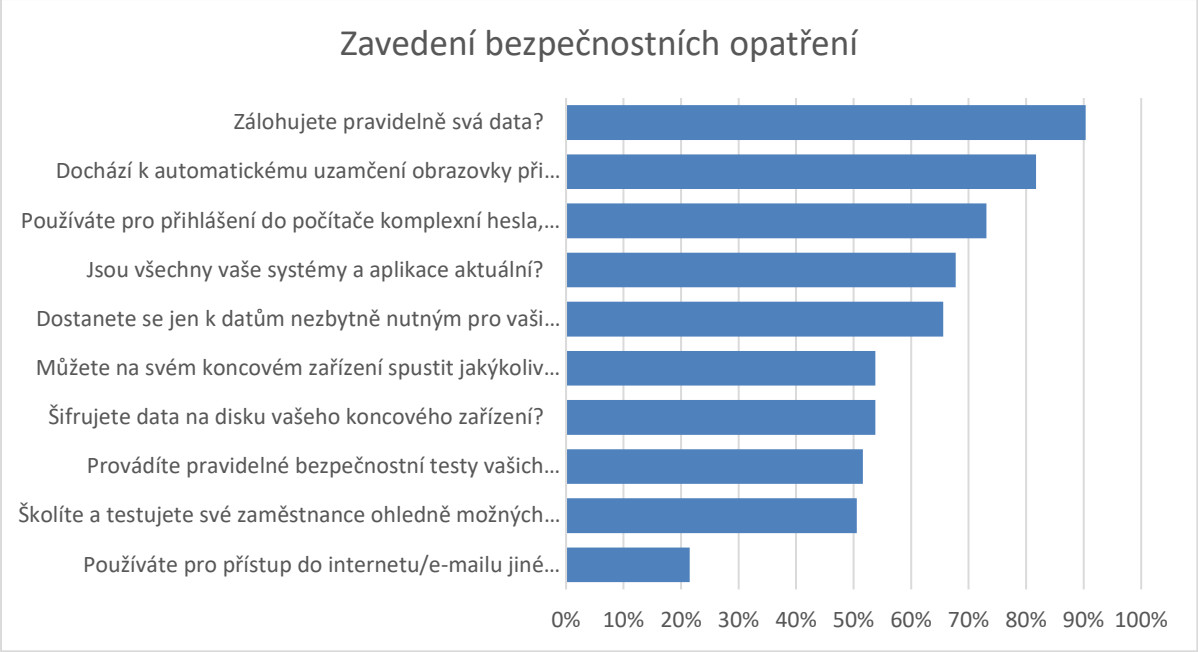
Další závěry

V následující části jsou uvedeny další závěry, ke kterým bylo možné na základě výsledku výzkumu dojít.

Přijatá opatření

Přestože zavedení základní sady bezpečnostních opatření by mělo představovat minimální náklad, tak ne všechny organizace ji zavedly.

Graf č. 1



Za negativní zjištění považujeme, že téměř čtvrtina firem (27 %) stále používá pro přihlášení do počítače slabá hesla. Sice by se mohlo zdát, že když tři čtvrtiny používají silná hesla nebo dvoufaktorovou autentizaci (73 %), tak je to dobrý výsledek, tak s přihlédnutím ke skutečnosti, že se skutečně jedná o základní a nejstarší bezpečnostní požadavek, tak tento výsledek nelze považovat za dobrý.

Alarmující je také skutečnost, že třetina firem (34 %) neřídí striktně přístup k datům, což je druhý nejstarší požadavek a zaměstnanci se tak dostanou i k datům,

ke kterým by se neměli dostat. A nejde jen o to, že by tohoto přístupu mohli zneužít, ale že v okamžiku, kdy dojde k napadení jejich stanice malwarem, tak malware může přistupovat ke stejným datům jako aktuálně přihlášený uživatel.

Rovněž zarážející je, že téměř polovina organizací (49 %) neprovádí účinnou bezpečnostní osvětu svých zaměstnanců, neověřuje účinnost těchto školení, a neprovádí ani pravidelné bezpečnostní testy svých systémů (48 %).

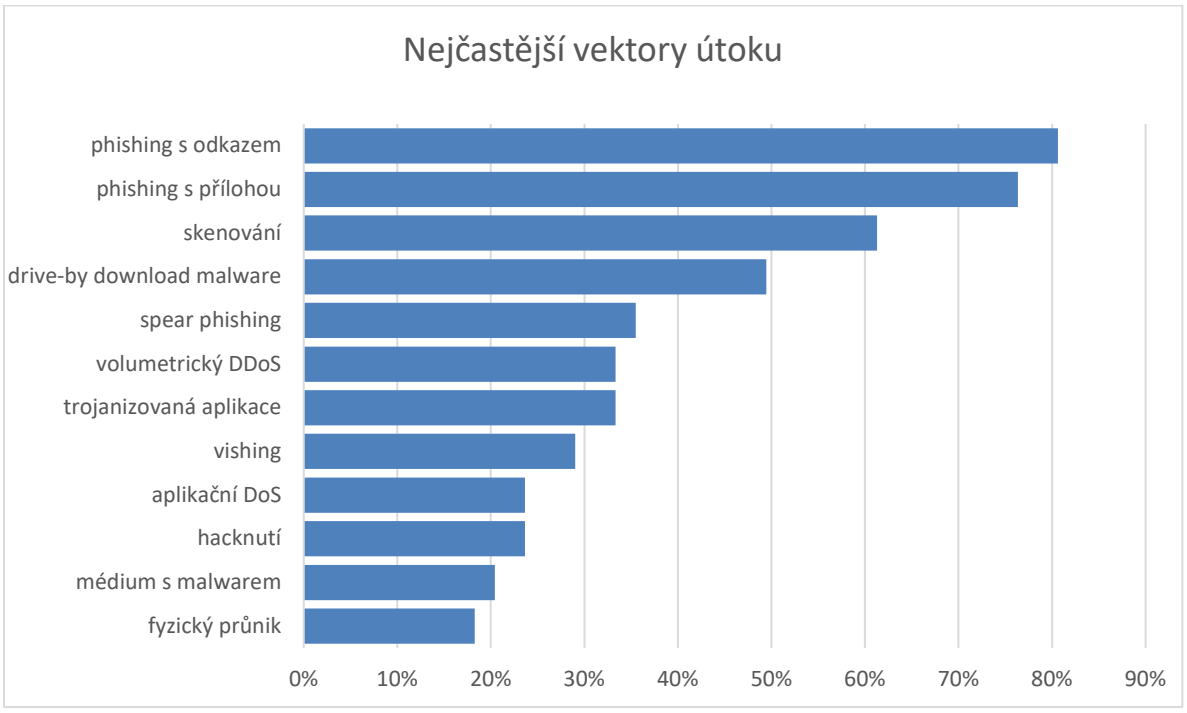
Určitou výzvu pak představuje oddělení informačního systému organizace od internetu a pošty, kterou se šíří nejvíce škodlivého kódu, protože více jak čtyři pětiny (78 %) firem umožňují svým zaměstnancům přistupovat z koncového zařízení jak do internetu a pošty, tak i do firemních systémů.

Jako pozitivní pak lze hodnotit, že drtivá většina firem (90 %) pravidelně zálohuje svá data, má nastaveno automatické uzamčení obrazovky po určité době nečinnosti (82 %), polovina firem (54 %) šifruje data na discích svých koncových zařízení, a téměř polovina (46 %) zakazuje svým zaměstnancům spustit na koncových zařízeních cokoliv a více jak dvě třetiny firem (68 %) jsou schopny udržovat své systémy aktuální a nasadit aktualizaci do několika málo týdnů od jejího zveřejnění.

Vektory útoku

Nejčastěji dochází k distribuci phishingových emailů s odkazem anebo přílohou, s tím se setkalo více jak 80 % organizací. Skenování systémů zaznamenaly dvě třetiny organizací. Téměř polovina se setkala s drive-by download malwarem. Poté následoval spear phishing, se kterým má zkušenost téměř 35 % organizací. Volumetrický DDoS zaznamenala přibližně třetina organizací. Čtvrtina se pak setkala vishingem, hackingem a aplikačním DoS. Pětina pak s médiem obsahujícím malware a o něco méně jich pak zaznamenalo fyzický průnik.

Graf č. 2



Závěr

Analýza odpovědí manažerů informační bezpečnosti působících v různě velkých organizacích v soukromém i veřejném sektoru národního hospodářství, provozující informační systémy různého stupně kritičnosti ukázala, že zde není patrný věcně významný vliv mezi velikostí, sektorem a dosaženou úrovní bezpečnosti a počtem a typem kybernetických útoků.

Nicméně byly identifikovány určité rozdíly mezi organizacemi působícími ve veřejném a soukromém sektoru co do zavedení vybraných bezpečnostních opatření, jako je např. šifrování dat na koncových zařízeních, použití technik sociálního inženýrství a obav z krádeže informací ze strany organizovaných skupin. Rovněž byly identifikovány rozdíly mezi organizacemi různých velikostí a jejich schopnostmi detekovat skenování jejich systémů, spouštět na koncových zařízeních libovolné programy, odolávat phishingu, ransomware a rovněž i jejich obavy ze sabotáže.

Můžeme vyslovit závěr, že se nepodařilo prokázat, že by četnost útoků a výše škody na těchto proměnných byla nějak závislá. Nicméně přesto je doporučujeme dále zjišťovat pro případ, že by situace v kyberprostoru v čase doznala změn a začaly by se zde určité rozdíly přeci jen projevovat.

Vzhledem k tomu, že se dále nepotvrdilo, že by všechny organizace měly zavedena základní bezpečnostní opatření, která byla ze strany bezpečnostních expertů shledána jako opravdu klíčová, neboť tato opatření zásadním způsobem snižují riziko narušení bezpečnosti, má tudíž i nadále smysl se ptát, zda má organizace příslušná bezpečnostní opatření zavedena či nikoliv a požadovat, aby byla implementována.

Literatura

ANDREW Preater. *Information as a commodity* – at #radliblon. Andrew Preater [online]. 3. červen 2014 [vid. 8. červen 2020]. Získáno z: https://www.preater.com/2014/06/03/information-as-a-commodity/

BLAHUŠ, Petr. Statistická významnost proti vědecké průkaznosti výsledků výzkumu. *Česká kinantropologie*. 2000, Vol. 4, No. 2, s. 53-72.

COHEN, Jacob. *Statistical Power Analysis for the Behavioral Sciences*. 2. vyd. Oxford: Routledge,1988. ISBN 978-0-8058-0283-2.

ELLIS, Paul D. *The Essential Guide to Effect Sizes: Statistical Power, Meta-Analysis, and the Interpretation of Research Results*. 1. vyd. New York: Cambridge University Press, 2010. 173 p. ISBN 978-0521142465.

HALLER, Martin. *Jak vypadá vyjednávání o výkupném u ransomware*. Martin Haller [online]. 11. květen 2020 [vid. 8. červen 2020]. Získáno z: https://martinhaller.cz/ransomware/jak-vypada-vyjednavani-o-vykupnem-u-ransomware/

HAMROZI, Petr. *V IT byl homeoffice běžný, po koronaviru dál poroste* [online]. [vid. 8. červen 2020]. Získáno z: https://www.nejbusiness.cz/zpravy/2020-05-06-v-it-byl-homeoffice-bezny-po-koronaviru-dal-poroste

HENDL, Jan. *Přehled statistických metod. Analýza a metaanalýza dat*. 1. aktual. vyd. Praha: Portál, 2004. ISBN 978-80-262-0981-2.

HOAX | *Metodika hodnocení míry nebezpečnosti* [online]. [vid. 8. červen 2020]. Získáno z: https://hoax.cz/cze/metodika-hodnoceni-miry-nebezpecnosti/

KIRK, E. Roger. *Statistics: An Introduction*. 5. vyd. Belmont: Thomson Higher, 2008. SBN 978-0-534-56478-0.

JIRÁSEK, Petr; NOVÁK, Luděk a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: první oficiální verze slovníku kybernetické bezpečnosti*. Vyd. 1. elektronické. Praha: Policejní akademie České republiky, 2012. ISBN 978-80-7251-377-2.

ŘEHÁK, Jan a Blanka ŘEHÁKOVÁ. *Analýza kategorizovaných dat v sociologii*. 1. vyd. Praha: Academia, 1986.

R E S U M É

Předložený článek prezentuje dílčí výsledky empirického výzkumu uskutečněného v minulém roce pracovníky PA ČR v Praze s cílem ověřit, zda existuje nějaká věcně významná závislost mezi velikostí organizace a sektorem organizace na jedné straně a bezpečnostními opatřeními, vektory útoku, incidenty, a obavami na straně druhé. Sběr dat byl proveden formou dotazníkového šetření mezi vybranými bezpečnostními experty nacházejícími se na pozici manažer informační bezpečnosti v různých organizacích v ČR. Vlastní analýza pak byla provedena za použití nástroje IBM SPSS Modeler, Statistics a PASS. Akceptovatelný věcně významný vliv byl ověřován s využitím měr datům adekvátních koeficientů asymetrické asociace a symetrického indexu věcné významnosti (Cohenovo w).

Klíčová slova: Kybernetické útoky, vektor útoku, bezpečnostní opatření, výzkumný předpoklad, klasifikační strom, koeficient asymetrické asociace, Goodman-Kruskalovo Tau, koeficient asymetrické asociace β, Cohenův index věcné významnosti w.

S U M M A R Y

ČERMÁK, Miroslav; KOVAŘÍK, Zdeněk: ISSUES OF CYBER-SECURITY DETERMINATION IN THE CONTEXT OF THE CZECH REPUBLIC

This paper describes partial results of empirical research conducted last year by PA CR staff in Prague. The main aim of this paper is to verify whether there is any material relationship between the size of the organization and the sector of the organization on the one hand and security measures, attack vectors, security incidents, and concerns on the other. Data for this research was collected in the form of a questionnaire survey from selected security experts in the position of information security manager in various organizations in the Czech Republic. The analysis itself was then performed using IBM SPSS Modeler, Statistics and PASS software tools. The acceptable materially significant effect was verified using measures of data corresponding to the coefficients of the asymmetric association and the symmetric index of material significance (Cohen's w).

Key words: Cyber-attack, attack vector, security measures, research hypothesis, classification scheme, coefficient of asymmetric association, Goodman-Kruskal Tau, coefficient of asymmetric association β, Cohen´s index of relevancy w.