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 úrovně kybernetické bezpečnosti v prostředí České republiky – 2. část

Předložený článek organicky navazuje na stať publikovanou v periodiku Bezpečnostní teorie a praxe Policejní akademie ČR v Praze v čísle 1 tohoto roku. První již publikovaný článek přinesl informace o výsledcích ověřování výzkumného předpokladu, jehož obsahem bylo zjištění doložitelného věcně významného vlivu působnosti sektoru (68,8 % soukromý sektor; 31,2 % veřejný sektor), ve kterém experti výběrového souboru působí a velikost jejich organizace (15,1 % mikropodnik, 14 % malý podnik do 50 osob, 20,4 % střední podnik do 250 osob a 50,5 % velký podnik nad 250 osob) na vybrané problémy kybernetické bezpečnosti.

V případě **působnosti sektoru** byl zjištěn akceptovatelný věcně významný vliv na čtyři položky: P01 - Šifrujete data na disku vašeho koncového zařízení?; P19 - Volal do vaší firmy někdo, kdo se vydával za někoho jiného a snažil se ze zaměstnanců vytáhnout informace?; P23 - Došlo u vás k výpadku proudu?; P51 - Obáváte se krádeže informací ze strany konkurence nebo organizovaných skupin? (APT).

V případě **působnosti velikosti organizace** byl zjištěn akceptovatelný věcně významný vliv na pět položek: P08 - Můžete na svém koncovém zařízení spustit jakýkoliv program nebo skript?; P11 - Zaznamenali jste skenování, inventarizaci, enumeraci ve vašich systémech?; P18 - Byl někomu z vašich zaměstnanců doručen spear phishing e-mail?; P33 - Došlo k zašifrování některých vašich dat ransomwarem?; P50 - Obáváte se sabotáže ze strany zaměstnance.

V tomto příspěvku se podíváme na výsledky ověřování výzkumného předpokladu vlivu odvětví národního hospodářství, ve které experti výběrového souboru působí, na posuzování škod, ke kterým u nich v souvislosti s kybernetickými útoky došlo a dále na posouzení jakých hrozeb se manažeři bezpečnosti v těchto odvětvích nejvíce obávají.

Vzhledem k tomu, že úvodní pasáž a metodologická část byla již zveřejněna v prvním článku, jakož i rozložení expertů výběrového souboru, není důvod je v předložené stati opakovat. Je však třeba hlouběji se podívat na přístup k předpokládané analýze závislostí mezi nominálními a ordinálními proměnnými a na zdůvodnění použitých hodnot měr asociace či věcné významnosti.

Postup ověřování výzkumného předpokladu 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 C5.0. Pro výpočet asymetrického koeficientu β byla využita utilita nadstandardně vytvořená pro systém SPSS. Cohenův index w byl zjištěn za pomoci programu NCSS PASS.

Použití rozhodovacích stromů pro hledání věcně významných závislostí

Před vlastní analýzou je potřebné se v rámci průzkumové analýzy dat podívat na jejich základní charakteristiky. Průzkumová analýza dat ukázala, že data porovnávaných skupin nemají ve většině případů normální rozdělení ani homogenní rozptyl. To však není na škodu věci, pokud se vezme do úvahy skutečnost, že záměrem je analýza dat kategorizovaných, nikoliv dat spojitých. Daný záměr tedy obrací pozornost na použití metod neparametrických.

Na tomto místě je třeba opět zdůraznit, že pokud se nepracuje s daty pořízenými náhodným výběrem, nelze zjištěné závěry zobecňovat na základní soubor. Jinak řečeno, statistická významnost výsledků analýzy ztrácí svou inferenční využitelnost a lze ji využívat pouze jako informaci o dostatečnosti rozsahu výběrového souboru pro analýzu dat. Získané závěry lze tedy vztahovat pouze k používanému výběrovému souboru.

Mezi stále používanější neparametrické metody analýzy dat patří **rozhodovací stromy**, které patří do skupiny nejúspěšnějších metod v této kategorii. Rozhodovací stromy si našly pevné místo v rámci tzv. **vytěžování dat či data miningu,** kde lze požadované parametry v datech v mnoha případech zřejmě těžko hledat.[1]

Co je velmi důležité a je třeba to zdůraznit, že **zejména slouží k podpoře rozhodování**. Otázka na charakter datového souboru (základní či výběrový) tu postrádá smysl. Analyzují se dostupná data (datové sklady nebo jejich části) a závěry slouží pro přijetí zdůvodněného rozhodnutí.

Použití rozhodovacích stromů má ještě další výhodu. Posiluje vizuální vnímání zjištěných odlišností a umožňuje velmi názorné posouzení rozdílů v procentuálním vyjádření odpovědí respondentů u jednotlivých kategorií odpovědí.

To značně posiluje rychlé porozumění smyslu odhalených vazeb (asociací). Při analýze bude nezávislá nominální proměnná zastoupena číselnou hodnotou, dle přiložené tabulky. Tímto přístupem bylo možné ušetřit místo pro zobrazení klasifikačních stromů, což by nebylo možné v případě uvedení celého názvu použitého odvětví národního hospodářství.

V našem případě je použití rozhodovacích stromů navíc vynuceno i skutečností danou velkou různorodostí nominální nezávislé proměnné ID02 - V jakém odvětví působí vaše organizace (daná proměnná je tvořena celkem sedmnácti možnostmi), jak je zobrazuje tabulka č. 1.

[1] Snad proto se někteří vyhranění odborníci ve statistice dívají na používání metod data miningu s jistou rezervou. Slouží pro analýzu velkých datových souborů, ale poradí si i se soubory malými.

Tabulka č. 1 – rozložení nezávislé proměnné ID02

1. Zemědělství, lesnictví a rybolov
2. Těžba a dobývání
3. Zpracovatelský průmysl
4. Výroba a rozvod elektřiny, plynu, tepla a klimatizovaného vzduchu
5. Velkoobchod a maloobchod, opravy a údržba motorových vozidel
6. Doprava a skladování
7. Ubytování, stravování a pohostinství
8. Informační a komunikační činnost
9. Peněžnictví a pojišťovnictví
10. Činnosti v oblasti nemovitostí
11. Profesní, vědecké a technické činnosti
12. Administrativní a podpůrné činnosti
13. Veřejná správa a obrana, povinné sociální zabezpečení
14. Vzdělávání (školy, univerzity)
15. Zdravotní a sociální péče
16. Kulturní, zábavní a rekreační činnost
17. Ostatní činnosti

Zjistit věcně významný vliv tak značně strukturované nezávislé nominální proměnné na ordinální závisle proměnnou lze nejadekvátněji dosáhnout právě s využitím rozhodovacích stromů za použití moderního algoritmu C5.0, který pro větvení stromu umí funkčně využít tzv. poměrný informační zisk, což je míra odvozená z entropie.

Poměrný informační zisk má za cíl zamezit vybrání atributů, které mají mnoho kategorií (náš případ 17 kategorií) a tudíž i větší entropii. U nich hrozí nebezpečí, že každá jejich kategorie bude zastoupena v případech pouze jednou nebo v malém počtu a zcela určovat cílovou třídu. Tudíž by měl tento atribut velký informační zisk. Například atribut jméno by mohl mít vysoký zisk, ale také sám o sobě bude mít vysokou entropii. Díky poměrnému informačnímu zisku je tento případ ošetřen.[1]

Použití měr koeficientu asociace, věcné významnosti a jejich zdůvodnění

V případech, kdy došlo k větvení rozhodovacího stromu (nalezení závislosti) byly absolutní četnosti v koncových uzlech přepočítány na hodnoty asymetrické asociace koeficientu β a symetrického Cohenova indexu w. V případě rozporných výsledků byly upřednostněny hodnoty asymetrického koeficientu asociace.

Míry asociace, které jsou založeny na modelech proporcionální redukce chyby (PRE) jsou přesné a uživatelsky srozumitelné. Patří mezi ně i koeficient β.[2] Podávají odpověď na otázku, o kolik může být lepší odhad jedné proměnné (závislé), jestliže jsou známy hodnoty jiné proměnné (nezávislé). Jiný, více používaný způsob interpretace říká, kolik procent rozptylu v závislé proměnné vysvětluje vliv nezávislé proměnné. Odpověď je vždy vyjádřena jako proporce v rozsahu od nuly do jedné, či procento v rozsahu od 0 % do 100 %.

[1] Blíže viz: 5.1 Rozhodovací stromy [online] [cit. 03. 6. 2020]. Dostupné z: https://sorry.vse.cz/~berka/docs/izi456/kap_5.1.pdf

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

S ohledem na to, že typ respondenta (prediktor) má nominální charakter a většina analyzovaných proměnných kybernetické bezpečnosti jsou ordinálního typu, bude v analýze zjišťována ordinální asymetrická asociace založená na asymetrickém koeficientu β (beta). Jde o regresní koeficient ordinální statistické závislosti. Jeho velikost signalizuje, o kolik % zlepšíme odhad znalosti rozložení odpovědí závisle ordinální proměnné (posuzovaný aspekt kybernetické bezpečnosti) poznáním rozložení nezávisle nominální proměnné (typ respondenta). Nyní se nabízí otázka, jak velká hodnota obou koeficientů je potřebná k nalezení akceptovatelné asociace. Uveďme stanovisko dvou významných českých statistiků, působících v sociálních vědách.

„Při aplikacích vždy vzniká otázka, jaká hodnota koeficientů je vysoká. Význam číselné hodnoty závisí na věcném významu proměnných a na modelu, který používáme. Jestliže očekáváme, že *A* je jedinou příčinou *B,* pak význam budou mít hodnoty vyšší než 0.6 nebo 0.7. Je-li *A* jednou z několika málo paralelních příčin heterogenity vzhledem k *B,* pak koeficienty 0.3, 0.5 budou vysoké. Je-li však *A* jednou z mnoha drobných příčin, pak i koeficient 0.1 či 0.05 je interpretovatelný. (Uvedené hodnoty jsou uvedeny subjektivně, a proto je nelze přijmout jednoznačně a s konečnou platností.)“[1]

Uvedená úvaha výše uvedených autorů naznačuje, že posouzení velikosti efektu asociace mezi proměnnými je subjektivní záležitostí výzkumníka při respektování věcného významu proměnných a modelu, který je použit.

V praktické analýze, při hledání skutečně akceptovatelných efektů se stále více dostává do popředí tzv. analýza věcné významnosti (effect of size). V tomto směru byly v odborné veřejnosti přijaty, i když ne s plným koncensem odborníků, určité konvence, které mají sloužit výzkumníkům v ne příliš jasných případech ve stanovení hranic (intervalů), kdy lze zjištěný efekt (skutečně zjištěný rozdíl) považovat z věcného hlediska za akceptovatelný. Následující tabulka č. 2 ukazuje přehled těchto koeficientů či indexů věcně významných rozdílů.[2]

[1] ŘEHÁK, Jan a Blanka ŘEHÁKOVÁ. *Analýza kategorizovaných dat v sociologii*. Praha: Academia, 1986, s. 252.

[2] 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. V tabulce č. 2 lze vidět kromě často používaného Cohenova indexu věcné významnosti pro nominální proměnné „w“ i kritizované koeficienty pro nominální proměnné fí, Cramerovo V a koeficient kontingence C (test Crosstabulation).

Tabulka č. 2

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

Z uvedených měr se s ohledem na svůj obsah nejvíce koeficientu β blíží čtverec ukazatele eta (η^2). Svými hodnotami 0,01 (malý efekt); 0,06 (střední efekt) a 0,14 (velký efekt) nabízí určité srovnávací hranice i pro koeficient β. Je však třeba mít na paměti, že jde o míru parametrického testu ANOVA.

Nyní je třeba se zamyslet nad modelovou situací, v níž budou posuzovány akceptovatelné věcně významné efekty.

Při posuzování vlivu názorů expertů výběrového souboru na zjišťované stránky kybernetické bezpečnosti je zřejmé, že jde pouze o jeden konkrétní vliv v celém mnohorozměrném sociálním poli. I když se vezme v úvahu, že kvalifikované stanovisko experta je pouze jedním z mnoha působících faktorů, jeho důležitost nelze podceňovat.

Pro posouzení akceptovatelného věcně významného vlivu dané nominální nezávislé proměnné na závislou ordinální proměnnou se tudíž jeví jako optimální použít pro dolní hranici věcně významného rozdílu hodnotu asymetrického koeficientu β ≥ 0,06 (6 % - střední věcně významný efekt).

Základní výzkumný předpoklad

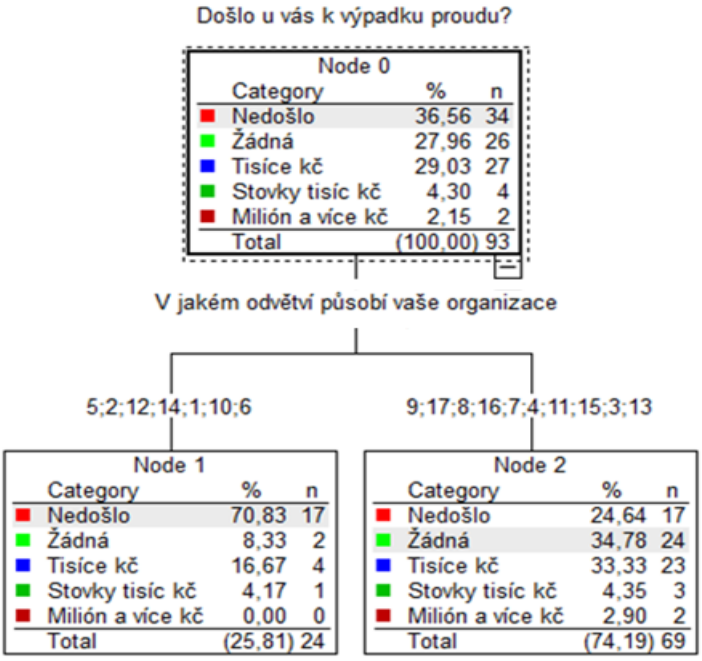
V rámci analýzy dat byl ověřován výzkumný předpoklad:

VP_0: Na odpovědi expertů výběrového souboru vztahující se k problematice kybernetické bezpečnosti zkoumaných organizací nebude mít akceptovatelný věcně významný vliv žádné ze sedmnácti zastoupených odvětví národního hospodářství, ke kterým experti výběrového souboru patří (koeficienty β ≥ 0,01; Cohenovo w ≥ 0,1).

Evidence analytických výsledků pro tvorbu závěru k ověřovanému výzkumnému předpokladu

V dalším textu je uvedena evidence dokládající závěr o věcně významném vlivu stanovisek expertů výběrového souboru odvětví národního hospodářství na dané aspekty dotazníkového šetření kybernetické bezpečnosti.

P23 - Došlo u vás k výpadku proudu?



Došlo u vás k výpadku proudu?	V jakém odvětví působí vaše organizace				
	První skupina	Druhá skupina	celkem	medián	dorvar
Nedošlo	+++	---	34	1,500	,500
Žádná	-	+	26	1,958	,142
Tisíce kč	o	o	27	1,913	,252
Stovky tisíc kč	o	o	4	1,833	,375
Milión a více kč	o	o	2	2,000	,000
celkem	24	69	93	1,826	,383

Hodnota koeficientu beta je 0,185 s 95% intervalem spolehlivosti (0,028; 0,343); (velká věcně významná asociace)[1]
Symetrický Cohenův index w = 0,431 (více než střední věcně významný efekt)

Výpadky proudu mohou být způsobeny vyšší mocí anebo se může jednat o následky cílených kybernetických útoků vedených na kritickou infrastrukturu státu a provozovatele přenosových soustav energie, na kterých jsou závislé i další organizace, některé více a některé méně. Tyto cílené útoky se přibližují k ČR, naposledy byly zaznamenány např. útoky na ENTSO-E.[2]

[1] Pod každým klasifikačním stromem je umístěna tabulka, která prostřednictvím křížků (+) ukazuje na dominance dané buňky s ohledem na četnosti zastoupených odpovědí a prostřednictvím znamének (-) naopak jejich inhibici (nedostatek). Značka (+++) značí velký přebytek daného typu odpovědí a (---) velký nedostatek daného typu odpovědí.

[2] European power grid organization hit by cyberattack. *WeLiveSecurity* [online]. 12. březen 2020 [vid. 4. červen 2020]. Získáno z: https://www.welivesecurity.com/2020/03/12/european-power-grid-organization-entsoe-cyberattack/

S výpadkem proudu se setkaly téměř dvě třetiny respondentů. Více jak čtvrtina (28 %) nezaznamenala žádnou ztrátu, ale další více jak čtvrtina (29 %) zaznamenala ztrátu ve výši několika tisíc korun, jen pár jednotek procent respondentů zaznamenalo ztrátu ve výši několika stovek tisíc (4,3 %) a více než milión (2,2 %) korun. Z výše uvedeného vyplývá, že výpadek proudu není hrozba, kterou by většina organizací musela okamžitě řešit, přesto tato hrozba představuje pro několik procent organizací hrozbu, která jim může způsobit poměrně vysokou škodu.

Ještě zajímavější pohled přináší výše uvedený strom, ze kterého je patrné, že některé organizace spadající do odvětví uvedených v Node 1 výpadek proudu nezaznamenaly vůbec (70,8 %) anebo jejich škoda byla minimální a naproti tomu z organizací, které spadají do odvětví uvedených v Node 2, nezaznamenala výpadek jen přibližně čtvrtina z nich (24,6 %), což může být dáno tím, že jejich citlivost na výpadek proudu je vzhledem k povaze jejich činnosti vyšší a rovněž vyšší je i podíl organizací, které utrpěly škodu ve výši několika tisíc korun (33,3 %) a pár procent z nich (2,9 %) pak dokonce škodu vyšší než milión korun.

V dalším výzkumu by bylo vhodné se zaměřit i na příčiny těchto výpadků, a zda byla přijata vhodná opatření k minimalizaci škod.

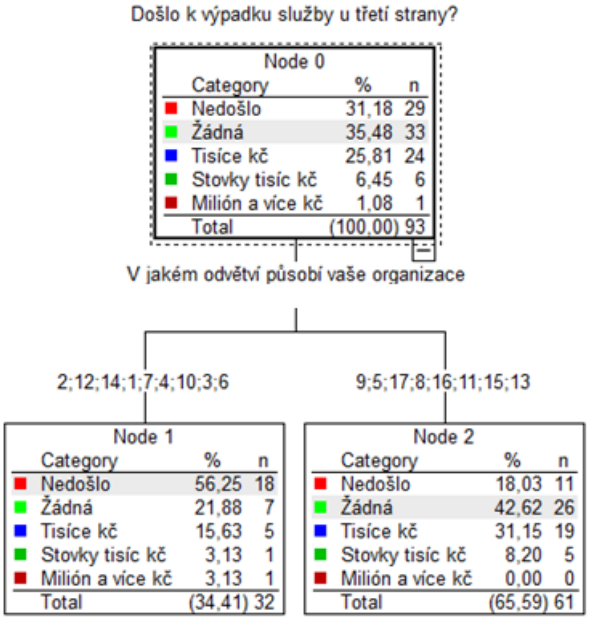
P24 - Došlo k výpadku služby u třetí strany?

Tak, jak je stále více činností outsourcováno, tak se organizace stávají více závislé na třetích stranách, které se rovněž stávají obětí kybernetických útoků, a počet těchto útoků roste.[1] Výpadek jejich služeb pak může mít negativní dopad na jejich podnikání a to podle toho, jak se činnost, kterou třetí strana vykonává, podílí na samotném hodnototvorném řetězci dané organizace.

Téměř jedna třetina (31,2 %) organizací se s výpadkem služeb třetí strany nesetkala, další více jak třetina (35,5 %) se s ním setkala, ale neutrpěla žádnou škodu a přibližně čtvrtina (25,8 %) pak utrpěla škodu ve výši několika tisíc korun. Jen pár procent organizací pak utrpělo škodu ve výši stovek tisíc (6,5 %) a jedno procento (1,1 %) pak škodu větší než jeden milión korun.

Když se podíváme, jakých organizací se toto týkalo, tak zjistíme, že zde máme organizace působící v odvětvích uvedených v Node 1, které jsou na třetích stranách závislé minimálně, více jak polovina z nich se s výpadkem služeb nesetkala (56,2 %), neutrpěla žádnou škodu (21,9 %) anebo se škoda pohybovala v řádu tisíců (15,6 %), případně pak u pár procent organizací (3,1 %) ve stovkách tisíc (3,1 %) nebo v miliónech (3,1 %).

[1] CONTINUUM. White Paper | Under Attack: The State of MSP Cybersecurity in 2019 [online]. [vid. 4. červen 2020]. Získáno z: https://page.continuum.net/resources/downloadables/white-paper/tf/under-attack-the-state-of-msp-cybersecurity-in-2019



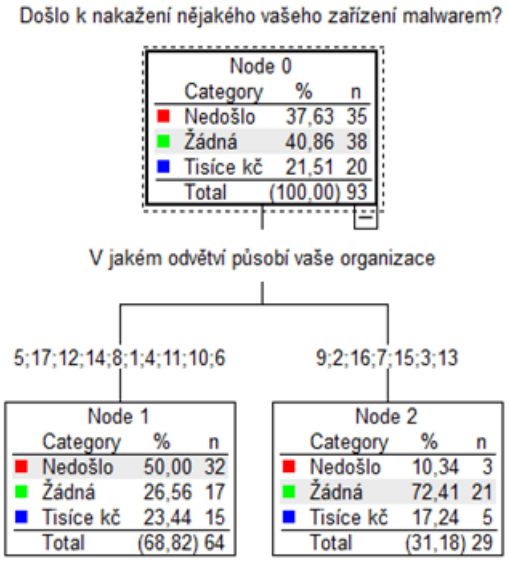
Došlo k výpadku služby u třetí strany?	V jakém odvětví působí vaše organizace				
	První skupina	Druhá skupina	celkem	medián	dorvar
Nedošlo	+++	---	29	1,533	,499
Žádná	o	o	33	1,911	,257
Tisíce kč	o	o	24	1,900	,278
Stovky tisíc kč	o	o	6	1,900	,278
Milión a více kč	o	o	1	2,000	,000
celkem	24	69	93	1,826	,383

Hodnota koeficientu beta je 0,121 s 95% intervalem spolehlivosti (-0,021; 0,264); (spíše velká věcně významná asociace)
Symetrický Cohenův index w = 0,429 (více než střední věcně významný efekt)

Organizace působící v odvětvích uvedených v Node 2 na tom byly, co se týče závislosti a škod, podstatně hůře. Jen necelá pětina (18 %) se s výpadkem služeb třetí strany nesetkala vůbec. A byť více jak dvě pětiny neutrpěly žádnou škodu (42,6 %), tak to na druhou stranu znamená, že k výpadku došlo, ale nebyl tak dlouhý anebo byla přijata odpovídající opatření k eliminaci škod, avšak téměř třetina organizací (31,1 %) utrpěla škodu ve výši několika tisíc korun a necelá desetina (8,2 %) pak dokonce ve výši několika stovek tisíc korun.

Výpadek služeb třetích stran nemusí být způsoben následkem kybernetického útoku, a přesto může způsobit značnou škodu. V dalším výzkumu by bylo vhodné se zaměřit i na příčiny těchto výpadků, a zda byla přijata vhodná opatření k minimalizaci škod.

P32 - Došlo k nakažení nějakého vašeho zařízení malwarem?



Došlo k nákažení nějakého vašeho zařízení malwarem?	V jakém odvětví působí vaše organizace				
	První skupina	Druhá skupina	celkem	medián	dorvar
Nedošlo	+++	---	35	1,047	,157
Žádná	---	+++	38	1,595	,494
Tisíce kč	o	o	20	1,167	,375
celkem	64	29	93	1,227	,429

Hodnota koeficientu beta je 0,204 s 95% intervalem spolehlivosti (0,048; 0,359); (velká věcně významná asociace)
Symetrický Cohenův index w = 0,452 (více než střední věcně významný efekt)

Hrozba nákazy generickým malwarem, obzvláště v případě plošně vedených útoků, se nevyhýbá žádné organizaci, nicméně více jak třetina (37,6 %) organizací byla schopna se malware úspěšně ubránit a detekovat jej, takže ke kompromitaci koncového zařízení nakonec nedošlo. Dvě pětiny (40,9 %) organizací pak byly napadeny, ale malware jim nezpůsobil žádnou škodu a více jak pětina (21,5 %) pak utrpěla škodu v řádu tisíců korun, což odpovídá minimálním nákladům na odstranění malware a obnovu koncového zařízení a dat a vyžaduje mít zavedený vyzrálý proces a funkční systém zálohy a obnovy dat.

Až polovina (50 %) organizací působících v odvětví uvedených v Node 1 byla schopna útok zastavit v počátku a v pozdější fázi pak více jak čtvrtina (26,6 %) z nich a necelá čtvrtina (23,4 %) pak utrpěla škodu ve výši tisíců korun.

Jen desetina organizací působících v odvětví uvedených v Node 2 zastavila útok již v počátku a téměř tři čtvrtiny (72,4 %) teprve až v další fázi, ale i to je dobrý výsledek, nicméně část z nich rovněž utrpěla škodu (17,2 %) v řádu tisíců.

Vidíme, že byť se tyto dvě skupiny organizací liší především v tom, v jaké fázi jsou schopny zachytit útok, tak obě skupiny utrpěly škodu v řádu tisíců korun a že

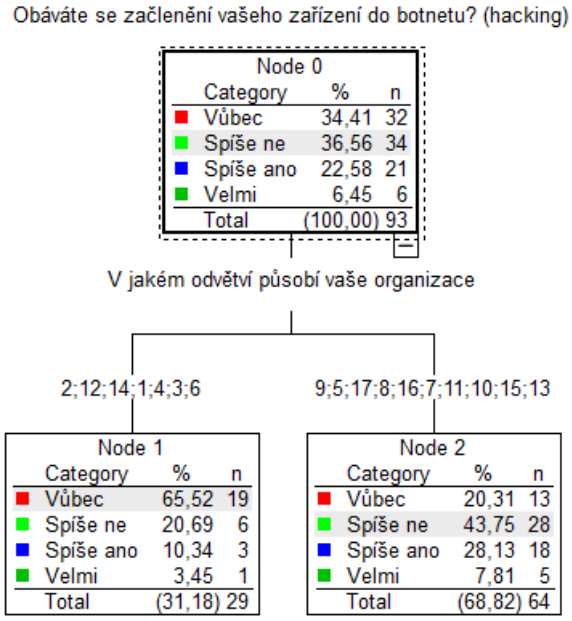
i generický malware může stále způsobit nějakou škodu, byť nepatrnou, a proto má antimalware řešení stále smysl.

Z rozhovoru s bezpečnostními experty, kteří situaci v kyberprostoru sledují od roku 2012, dále vyplynulo, že nejúčinnější jsou v tomto případě řešení od českých výrobců, která jsou schopna detekovat plošně vedené útoky na české uživatele, především díky vysoké tržní penetraci a schopnosti včas detekovat a reagovat na malware, který se našem území aktuálně šíří a to v řádu hodin, maximálně jednotek dnů, zatímco řešení zahraniční provenience jsou schopny stejný malware detekovat až po několika dnech a v mnoha případech až po týdnu.

Dílčí zjištění

Pokud jde o hrozby a způsobené škody zkoumané v rámci tohoto výzkumu, tak z rozhovoru s manažery informační bezpečnosti dále vyplynulo, že neví, jak přesně mají škodu počítat, a že způsob výpočtu škody se organizace od organizace liší.

P45 - Obáváte se začlenění vašeho zařízení do botnetu? (hacking)



Obávát se se začlenění vašeho zařízení do botnetu? (hacking)	V jakém odvětví působí vaše organizace				
	První skupina	Druhá skupina	celkem	medián	dorvar
Vůbec	+++	---	32	1,559	,498
Spíše ne	o	o	34	1,914	,251
Spíše ano	o	o	21	1,917	,245
Velmi	o	o	6	1,900	,278
celkem	24	69	93	1,826	,383

Hodnota koeficientu beta je 0,122 s 95% intervalem spolehlivosti (-0,02; 0,263); (spíše velká věcně významná asociace)
Symetrický Cohenův index w = 0,442 (více než střední věcně významný efekt)

V okamžiku, kdy je zařízení začleněno do botnetu, a tato hrozba vzrostla, neboť oproti roku 2018 reportuje např. Spamhaus nárůst C&C serverů o 71,5 %, tak může být pronajato nejen k dalšímu útoku, ale např. i k průmyslové špionáži, jak uvádí Bederna[1] a ve výsledku může organizace utrpět značnou škodu. Více jak třetina (34,4 %) organizací se této hrozby neobává vůbec, spíše ne (36,6 %), spíše ano (22,6 %) a velmi se obávají jen pouhá procenta (6,5 %) organizací.

Zajímavé je, že z organizací působících v odvětvích uvedených v Node 1, se této hrozby vůbec neobávají téměř dvě třetiny (65,5 %) organizací, spíše ne pak pětina organizací (20,7 %), spíše ano pak desetina (10,3 %) a velmi se obává jen pár procent (3,4 %) organizací. Z organizací spadajících do odvětví národního hospodářství uvedených v Node 2 se této hrozby vůbec neobává jen pětina (20,3 %) z nich, spíše ne pak více jak dvě pětiny (43,8 %), spíše ano pak téměř třetina (28,1 %) a velmi jen několik málo procent (7,8 %).

Skutečnost, že se druhá skupina obává začlenění do botnetu více, je dáno nejspíš tím, že si uvědomují, že by ji tato skutečnost mohla poškodit, což vzhledem k předmětu jejich činností dává smysl.

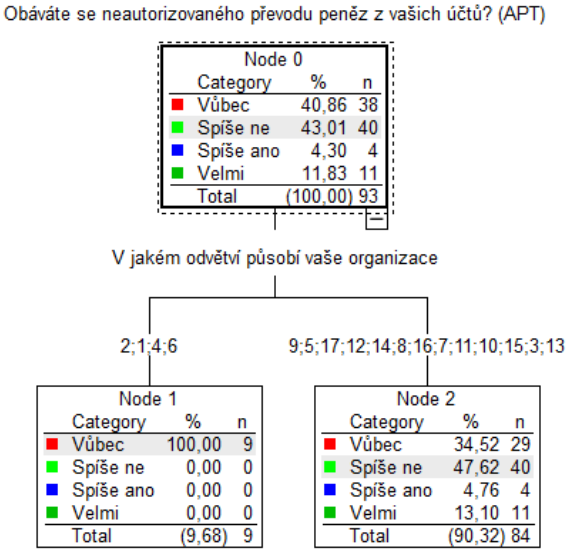
P47 - Obáváte se neautorizovaného převodu peněz z vašich účtů? (APT)

Neautorizovaný převod finančních prostředků se řadí spolu s kompromitací systému a jeho ovládnutím a ransomware k hrozbám, které mohou způsobit největší škodu. K masivním útokům na klienty největších českých bank, kterými jsou jak domácnosti, tak i firmy, dochází od roku 2013, a že počty těchto útoků rostou, uvádí i Česká bankovní asociace.[2]

Dvě pětiny organizací se přesto této hrozby neobává vůbec (40,9 %) anebo spíše ne (43 %) a spíše ano se obává jen pár jednotek procent (4,3 %) a velmi se obává přibližně desetina (11, 8 %). Zajímavější však je, jak se liší obavy podle odvětví, do jakého tyto organizace patří. Všechny organizace uvedené v Node 1 nemají obavu vůbec (100 %), zatímco pokud jde o organizace uvedené v Node 2, tak se této hrozby vůbec neobává více jak třetina organizací (34,5 %), spíše ne pak téměř polovina (47,6 %) a spíše ano jednotky procent (4,8 %) a velmi se této hrozby obává více jak desetina organizací (13,1 %).

[1] BEDERNA, Z.; SZADECZKY, T. Cyber espionage through Botnets. *Secur J 33,* 43-62 (2020). https://doi.org./10.1057/s41284-019-00194-6.

[2] Kyberbezpečnost a index bezpečnosti 2019. *Česká bankovní asociace* [online]. [vid. 4. červen 2020]. Získáno z: https://cbaonline.cz

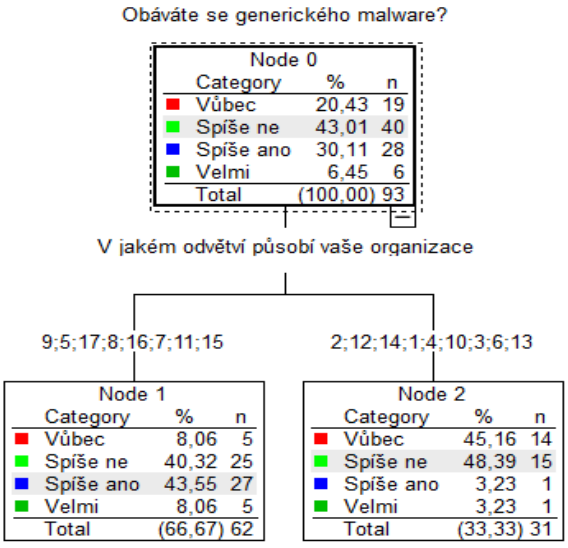


Obáváte se neautorizovaného převodu peněz z vašich účtů? (APT)	V jakém odvětví působí vaše organizace				
	První skupina	Druhá skupina	celkem	medián	dorvar
Vůbec	+	-	38	1,674	,478
Spíše ne	o	o	40	1,894	,289
Spíše ano	o	o	4	1,833	,375
Velmi	o	o	11	1,950	,165
celkem	24	69	93	1,826	,383

Hodnota koeficientu beta je 0,073 s 95% intervalem spolehlivosti (-0,031; 0,176); (více než střední věcně významná asociace)
Symetrický Cohenův index w = 0,394 (více než střední věcně významný efekt)

Tuto skutečnost si vysvětlujeme tím, že organizace spadající do první skupiny se s tímto útokem doposud nesetkaly a neví ani o tom, že by se obětí staly nějaké jiné organizace působící ve stejném odvětví. Mezi manažery stále převládá názor, že se jedná o cílené útoky, nikoliv o plošné.

P48 - Obáváte se generického malware?



Obáváte se generického malware?	V jakém odvětví působí vaše organizace				
	První skupina	Druhá skupina	celkem	medián	dorvar
Vůbec	---	+++	19	1,821	,388
Spíše ne	o	o	40	1,300	,469
Spíše ano	+++	---	28	1,019	,069
Velmi	o	o	6	1,100	,278
celkem	62	31	93	1,250	,444

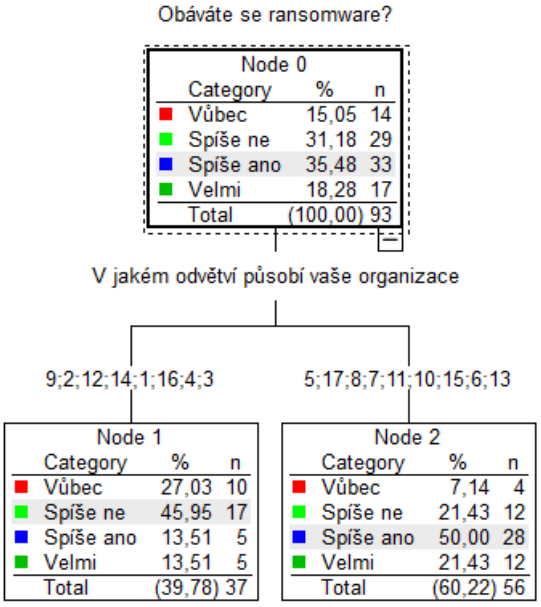
Hodnota koeficientu beta je 0,281 s 95% intervalem spolehlivosti (0,122; 0,44); (velká věcně významná asociace)
Symetrický Cohenův index w = 0,530 (velký věcně významný efekt)

Generického malware se velmi obává jen pár procent organizací (6,5 %), spíše ano pak téměř třetina (30,1 %), spíše ne více jak dvě pětiny (43 %) a vůbec pak pětina (20,4 %). Skutečnost, že dvě třetiny organizací se generického malware neobávají, si lze vysvětlit tak, že si již na něj zvykly, neboť se s generickým malwarem setkávají po celou dobu své existence.

Vyprofilovaly se zde však dvě skupiny organizací, které se podstatně liší v tom, jak vnímají obavu z generického malware. Organizace uvedené v Node 1 se generického malware neobávají vůbec jen v několik málo procentech (8,1 %).

Organizací uvedených v Node 2, které se vůbec neobávají generického malware, je mnohonásobně více (45,2 %), což si lze vysvětlit tak, že se necítí býti ohroženi generickým malwarem, neboť jsou přesvědčeni, že se jich tento problém buď netýká anebo že jsou vůči němu dostatečně chráněni pomocí stávajících bezpečnostních opatření.

P49 - Obáváte se ransomware?



Obáváte se ransomware?	V jakém odvětví působí vaše organizace: První skupina	Druhá skupina	celkem	medián	dorvar
Vůbec	+++	---	14	1,200	,408
Spíše ne	o	o	29	1,841	,366
Spíše ano	-	+	33	1,931	,213
Velmi	o	o	17	1,893	,291
celkem	24	69	93	1,826	,383

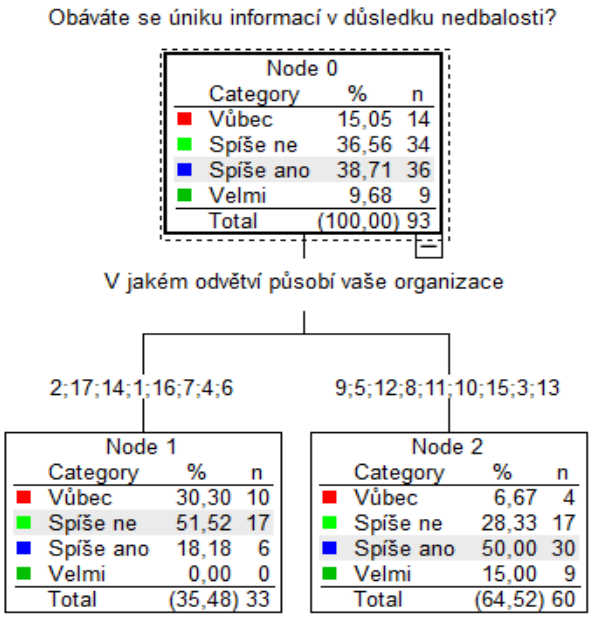
Hodnota koeficientu beta je 0,205 s 95% intervalem spolehlivosti (0,017; 0,393); (velká věcně významná asociace)
Symetrický Cohenův index w = 0,455 (téměř velký věcně významný efekt)

Ransomware představuje nebezpečí pro každou organizaci, protože každá organizace spravuje osobní údaje svých zaměstnanců anebo klientů a především pak pro ty organizace, které nemají fyzicky oddělené zálohy od sítě a netestují je. Obava z ransomware je obecně větší, než z generického malware, neboť zde si již většina respondentů dovede představit nejhorší možnou škodu, která by jejich organizacím mohla vzniknout a také škoda z ransomware je zpravidla výrazně vyšší, než z ostatního generického malware.

Ransomware se velmi obává téměř pětina organizací (18,3 %) a spíše ano pak více jak třetina (35,6 %). Vznikly zde dvě skupiny organizací s rozdílným vnímáním této hrozby. Organizace uvedené v Node 1 se ransomware obávají výrazně více, polovina (50 %) se vyjádřila, že spíše ano a velmi pak více jak pětina (21,4 %), zatímco ve druhé skupině organizací uvedených v Node 2 se jen více jak desetina organizací (13,5 %) vyjádřila jako spíše ano nebo velmi (13,5 %).

Vysvětlujeme si to tím, že organizace spadající do druhé skupiny jsou organizace, které se již v minulosti s ransomware setkaly anebo se s ním setkaly v době vyplňování dotazníku a tak byly touto skutečností silně ovlivněny stejně jako zprávami v médiích, které o této hrozbě rovněž informovaly.

P53 - Obáváte se úniku informací v důsledku nedbalosti?



Obáváte se úniku informací v důsledku nedbalosti?	V jakém odvětví působí vaše organizace				
	První skupina	Druhá skupina	celkem	medián	dorvar
Vůbec	++	--	14	1,200	,408
Spíše ne	+	-	34	1,500	,500
Spíše ano	--	++	36	1,900	,278
Velmi	-	+	9	2,000	,000
celkem	33	60	93	1,725	,458

Hodnota koeficientu beta je 0,232 s 95% intervalem spolehlivosti (0,078; 0,386); (velká věcně významná asociace)
Symetrický Cohenův index w = 0,481 (téměř velký věcně významný efekt)

Pokud jde o únik informací z nedbalosti, tak zde se této hrozby obává téměř polovina respondentů, spíše ano více jak třetina (38,7 %) a velmi pak necelá desetina (9,7 %).

Z odpovědí jednotlivých respondentů vyplývá, že se zde vyprofilovaly dvě skupiny organizací. V první skupině, do které patří organizace uvedené v Node 1, se této hrozby neobává vůbec celá třetina (30, 3 %) respondentů a spíše ne pak více jak polovina (51,5 %) respondentů. Naproti tomu ve druhé skupině, kam lze zařadit organizace uvedené v Node 2, se jen pouhých několik procent (6,7 %) z nich této hrozby neobává vůbec a necelá třetina respondentů (28,3 %) spíše ne.

Důvod, proč tomu tak je, si vysvětlujeme tím, že druhá skupina organizací disponuje know-how a informacemi, které mají na trhu větší hodnotu, a tudíž i jejich obava je větší.

Dílčí zjištění

Na Obrázek č. 1 je zachycena podobnost mezi jednotlivými odvětvími.

Obrázek č. 1

Node 1

Odvětví	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
P23	1	2			5	6				10		12	14				
P24	1	2	3	4		6	7			10		12	14				
P32	1			4	5	6		8		10	11	12	14				17
P45	1	2	3	4		6						12		14			
P47	1	2		4		6											
P48					5		7	8	9		11				15	16	17
P49	1	2	3	4					9			12		14		16	
P53	1	2		4		6	7							14		16	17

Node 2

Odvětví	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
P23		3		4			7	8			9	11	13		15	16	17
P24					5			8			9	11	13		15	16	17
P32	2	3					7				9		13		15	16	
P45					5		7	8	9	10	11		13		15	16	17
P47			3		5		7	8	9	10	11	12	13	14	15	16	17
P48	1	2	3	4		6				10		12	13	14			
P49					5	6	7	8		10	11		13		15		17
P53			3		5			8	9	10	11	12	13		15		

Zeleně označená odvětví (1, 6, 10, 12, 14) v Node 1 jsou v kontextu hodnocení odpovědí na dané otázky stejné a mohly by se sdružit stejně jako odvětví v Node 2 (9, 13, 15, 16).

Závěr

Analýza odpovědí manažerů informační bezpečnosti působících v různých odvětvích ukázala, že zde jsou určité rozdíly mezi odvětvími, které by se měly v rámci hodnocení rizikovosti klienta vzít v potaz.

Naši pozornost upoutala především škoda vyplývající z výpadku proudu a služeb třetích stran, generický malware a dále pak obava ze začlenění zařízení organizace do botnetu, neautorizovaného převodu peněz, generického malware, ransomware a únik informací z nedbalosti, kde lze najít mezi organizacemi určité rozdíly.

Vytváří se zde různé skupiny, které vykazují společné charakteristiky co do výše škod anebo vyjádřených obav z některých kybernetických hrozeb. Zde je ale v zájmu objektivity nutné připustit, že rozdílné obavy mohou být způsobeny i rozdílnými zkušenostmi.

Přesto nelze ignorovat fakt, že manažeři spolu komunikují a sdružují se v nejrůznějších profesních a sociálních skupinách, kde sdílí své obavy a tak se

vzájemně ovlivňují. A nepochybně zde značnou roli hrají i média, která rovněž utváří jejich názor filtrováním a skladbou svých zpráv.

V dalším výzkumu by bylo vhodné se zaměřit rovněž na závislost mezi mírou obavy a úrovní zavedených bezpečnostních opatření.

Analýza dále ukázala, že zde jsou organizace, které byť působí v různých odvětvích, tak vykazují určité společné charakteristiky, např. z pohledu resistence vůči škodám anebo sdílením obdobných obav.

Literatura

5.1 Rozhodovací stromy [online] [cit. 03. 6. 2020]. Dostupné z: https://sorry.vse.cz/~berka/docs/izi456/kap_5.1.pdf

BEDERNA, Z.; SZADECZKY, T. Cyber espionage through Botnets. *Secur J 33,* 43-62 (2020). https://doi.org./10.1057/s41284-019-00194-6.

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.

CONTINUUM. White Paper | Under Attack: The State of MSP Cybersecurity in 2019 [online]. [vid. 4. červen 2020]. Získáno z: https://page.continuum.net/resources/downloadables/white-paper/tf/under-attack-the-state-of-msp-cybersecurity-in-2019

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. ISBN 978-0521142465. 173 p.

European power grid organization hit by cyberattack. *WeLiveSecurity* [online]. 12. březen 2020 [vid. 4. červen 2020]. Získáno z: https://www.welivesecurity.com/2020/03/12/european-power-grid-organization-entsoe-cyberattack/

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

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

Kyberbezpečnost a index bezpečnosti 2019. *Česká bankovní asociace* [online]. [vid. 4. červen 2020]. Získáno z: https://cbaonline.cz

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 isbn978-80-7251-377-2.

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 a zaměřuje se na expertní posouzení závislosti subsumace organizace do příslušného odvětví a její odolnosti vůči kybernetickým útokům a vyjádřeným obavám z těchto útoků. Akceptovatelný věcně významný vliv byl ověřován s využitím měr datům adekvátních koeficientů asymetrické asociace a symetrického indexu věcné významnosti (Cohenovo w). Výsledky analýzy ukázaly, že se odpovědi respondentů patřící do různých odvětví na zadané vybrané otázky věcně významně odlišují jen v některých specifických případech, což nás vede k závěru, že subsumace organizace do příslušného odvětví není z pohledu hodnocení úrovně bezpečnosti rozhodující.

Klíčová slova: Kybernetické útoky, odvětví, obavy, výzkumný předpoklad, klasifikační strom, algoritmus C5.0, koeficient asymetrické asociace β, symetrický 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 – PART TWO

This paper describes partial results of empirical research carried out this year by the staff of the PA CR in Prague. The main aim of this research was to present a proposal for a rapid assessment of cyber security resilience in a selected organization. There were interviewed ninety-three respondents working in the position of information security manager in various organizations in the Czech Republic. The research focused on the experts' assessment of the dependence of the organization's subsumation into a certain group of industry. The acceptable materially significant effect was verified by using measures of data corresponding to the coefficients of the asymmetric association and the symmetric index of material significance (Cohen's w). The results of the analysis showed that the answers of respondents belonging to different industries to the selected questions differ significantly only in few specific cases.

Key words: Cyber-attack, industry, fear, research hypothesis, classification scheme, algorithm C5.0, coefficient of asymmetric association β, symmetric Cohen´s index of relevancy w.