www.pwc.cz

Kyberbezpečnost a my

Průzkum na téma aspekty vzdělávání zaměstnanců v oblasti kyberbezpečnosti

2017

pwc

Tate International

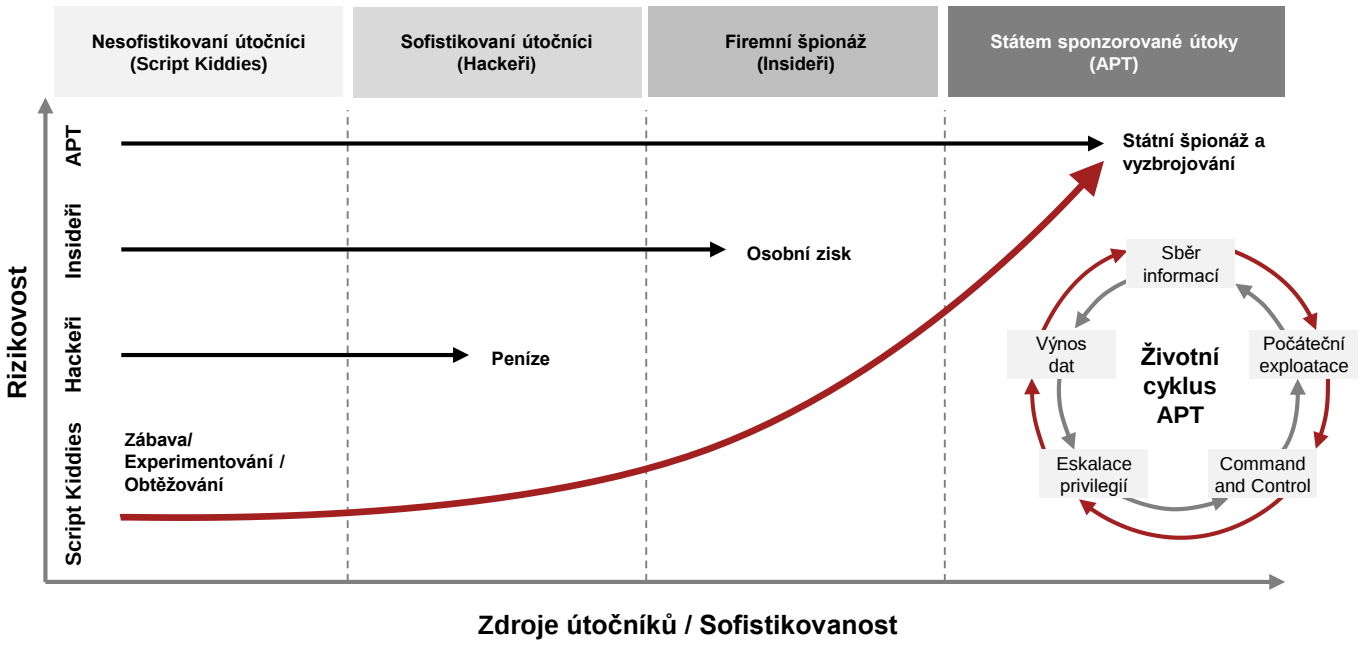
Úvod

V posledních letech se výrazně zvýšil počet kybernetických útoků, které využívají nejzranitelnější článek – lidi. V reakci na tento trend provedl PwC CyberSecurity Team průzkum *Kyberbezpečnost a my* ve spolupráci s TATE International.

Jsme velice rádi za možnost vám touto cestou představit výsledky tohoto průzkumu, které potvrzují, že v oblasti zvyšování kompetencí zaměstnanců i managementu existuje prostor pro zlepšení.

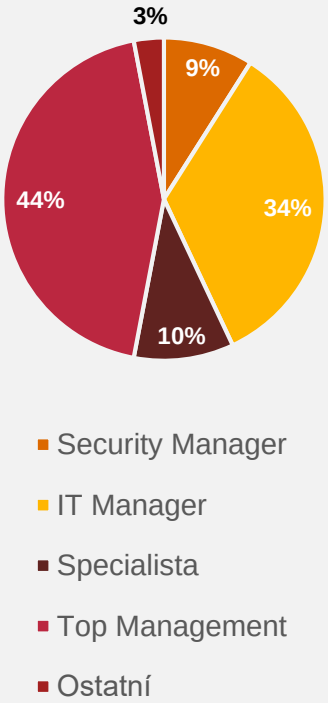
Každá společnost je jedinečná a hledá vlastní ideální cestu k zajištění bezpečnosti. Zároveň má každá své unikátní techniky a postupy, jejichž využitelnost a funkčnost závisí na prostředí. Zásadním měřítkem pro výsledek celého snažení je, jak moc pracovníci rozumí tématu a jak se budou chovat při případném útoku.

Věříme, že vám tento materiál bude inspirací pro další rozvoj vzdělávání v oblasti bezpečnosti ve vaší společnosti a usnadní rozhodování, jakým směrem se ubírat.



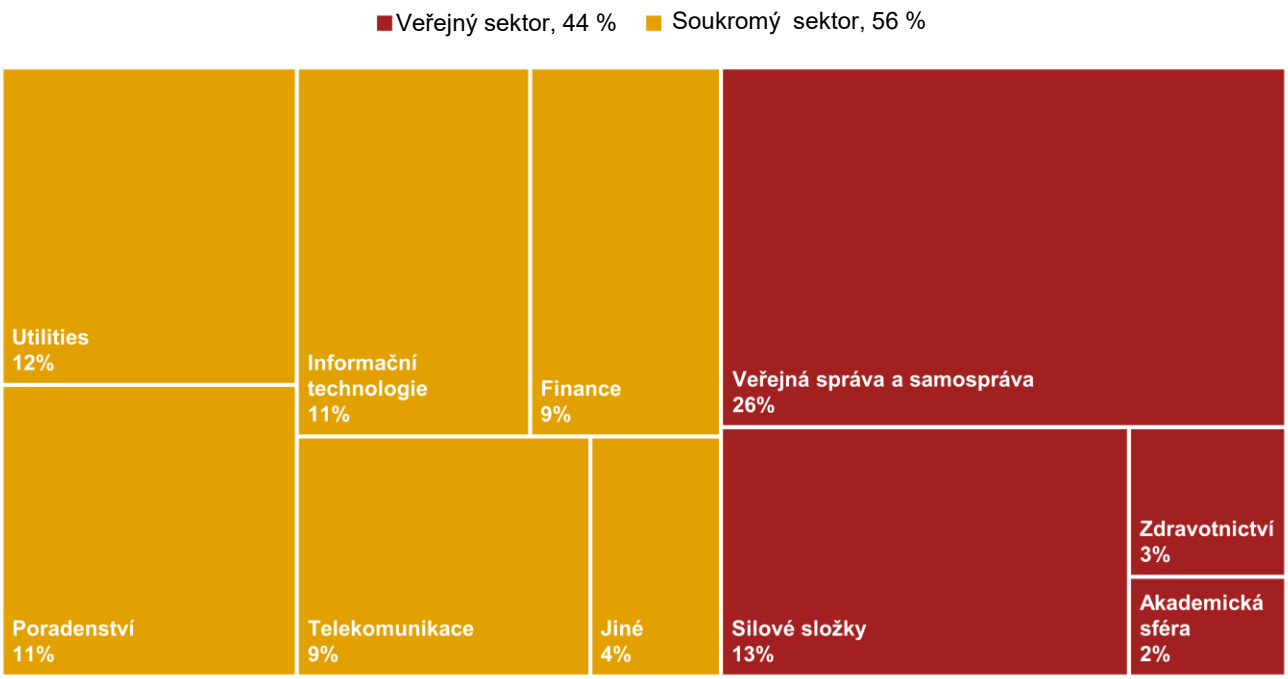
Zdroj: ISACA, Responding to Targeted Cyberattacks, USA, 2013

O průzkumu



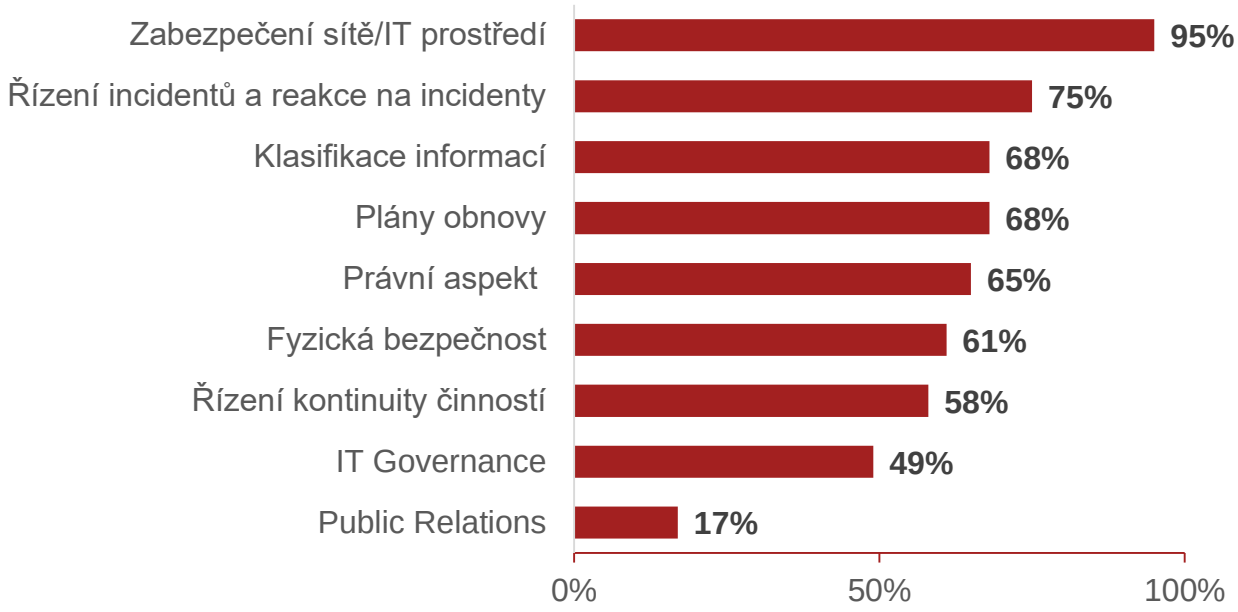
Průzkum *Kyberbezpečnost a my*, realizovaný společně s TATE International, byl zaměřen na různé aspekty vzdělávání zaměstnanců v oblasti kyberbezpečnosti a na subjektivní vnímaní přínosů tohoto úsilí respondenty průzkumu. Zároveň jsme se ptali, zda a jak probíhá spolupráce dotazovaných organizací s *Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB)*.

Dotazníkového šetření se zúčastnilo celkem 104 osob. Respondenti pocházejí z různých oblastí soukromého a veřejného sektoru, přičemž drtivá většina pracuje na manažerské pozici (celkem 87 % dotazovaných). Otázky, které jsme jim položili, mají pomoci k získání přehledu o aktuální úrovni a směřování vzdělávaní zaměstnanců v rámci ČR.



Výsledky průzkumu

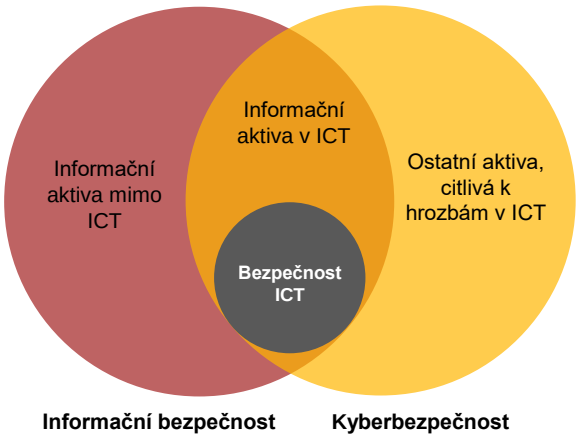
Co všechno podle vás spadá do kyberbezpečnosti?



Z výsledků vyplývá, že pro většinu dotazovaných kyberbezpečnost představuje spíše technické aspekty spojené s preventivními opatřeními a technickou bezpečností ICT prostředí. Na druhou stranu pouze malá část respondentů (7 %) zahrnuje do této problematiky další související oblasti.

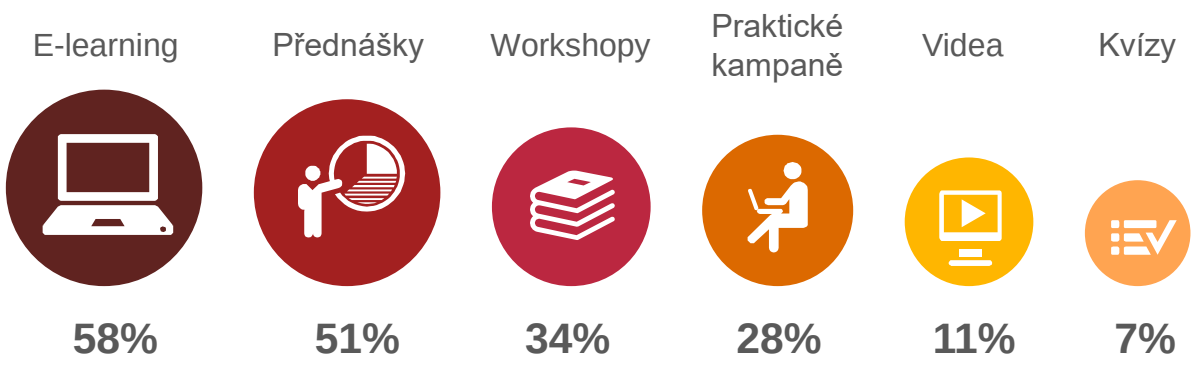
Mezi tyto oblasti patří:

- personální bezpečnost,
- interní řídící dokumentace,
- rodina standardů ISO 27k,
- krizové řízení,
- PDCA cyklus,
- ochrana osobních údajů.



Jeden z možných pohledů na rozdíl mezi informační bezpečností a kyberbezpečností

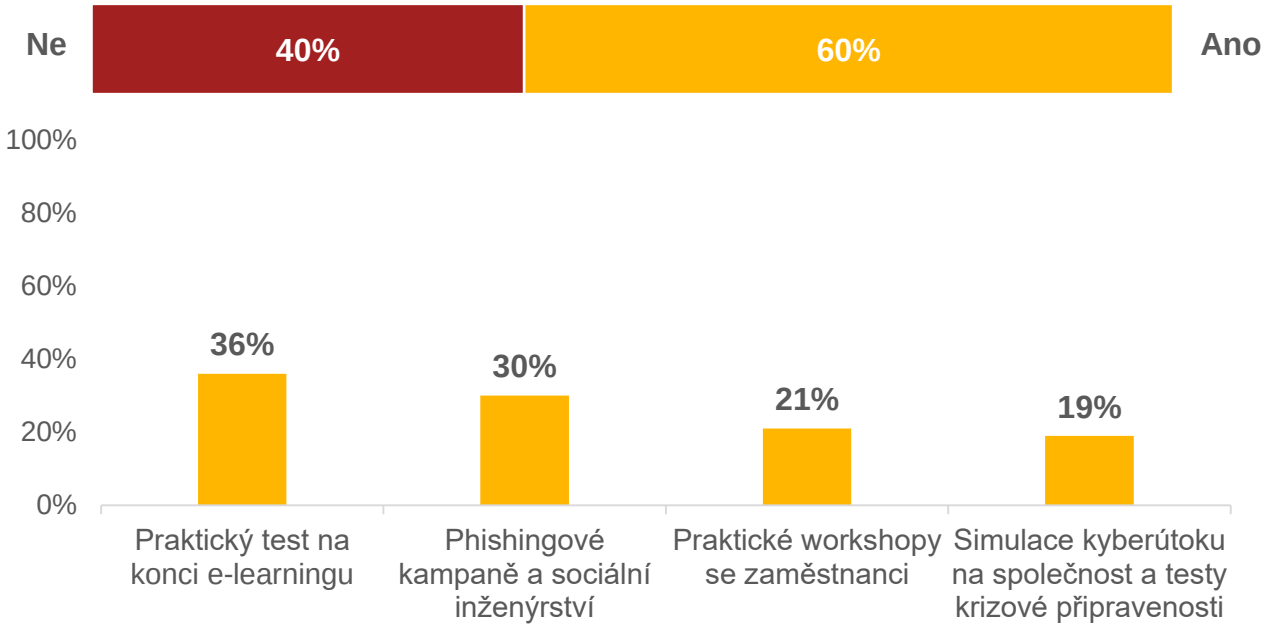
Jaké typy školení se využívají pro vzdělávání vašich zaměstnanců v oblasti kyberbezpečnosti?



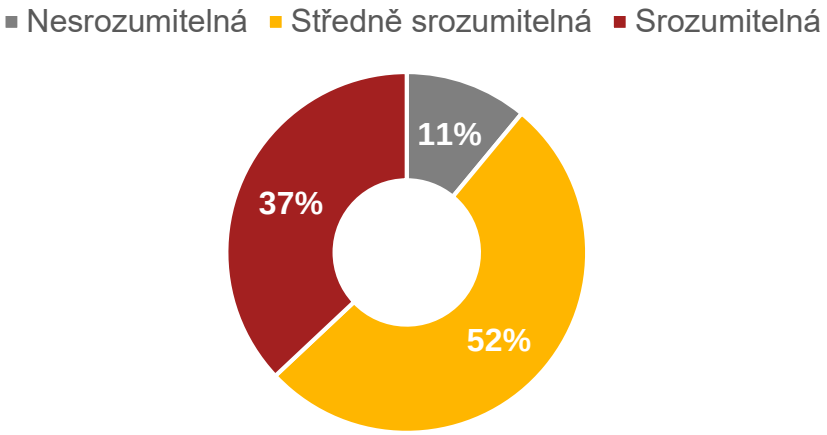
Ze získaných dat je zřejmé, že 61 % organizací používá ke školení zaměstnanců klasická prezenční školení formou workshopů a přednášek. Zhruba stejné zastoupení mají e-learningová školení. Minimálně jednu z těchto klasických forem školení využívá 81 % firem.

Trendem na trhu jsou nové formy školení: praktické simulace útoků, gamifikace nebo alespoň různé interaktivní testy. Z grafu níže je vidět, že některou z forem praktického tréninku zahrnuje do svých vzdělávacích plánů až 60 % společností. Příklady typů praktických školení dostupných na trhu jsou uvedeny na následující stránce.

Vybavujete si absolvování praktických školení souvisejících s kyberbezpečností?



Jsou školení kyberbezpečnosti dle vašeho mínění vašim zaměstnancům srozumitelná?



Tato otázka se soustředila na subjektivní vnímání srozumitelnosti školení zaměstnanci. Jednou z možností, jak srozumitelnost školení zvýšit, je větší využití praktických tréninků, kde je prakticky okamžitá zpětná vazba.

Příklady praktických tréninků

Phishingové kampaně

- Možnost využití pro pokročilé ověření získaných znalostí.
- Mají významný vzdělávací dopad.
- Počet zaměstnanců, kteří podlehnou útočníkům, se v každém kole snižuje.

Test sociálním inženýrstvím

- Pro pokročilé ověření odolnosti organizace proti některým útokům.
- Praktická demonstrace možností útočníků.

Game of Threats™

- Praktická ukázka simulace kybernetického útoku a obrany.
- Klientský tým složený ze specialistů i managerů má příležitost vyzkoušet si obranu i útok, a tím si následně snáze představit uvažování útočníka.

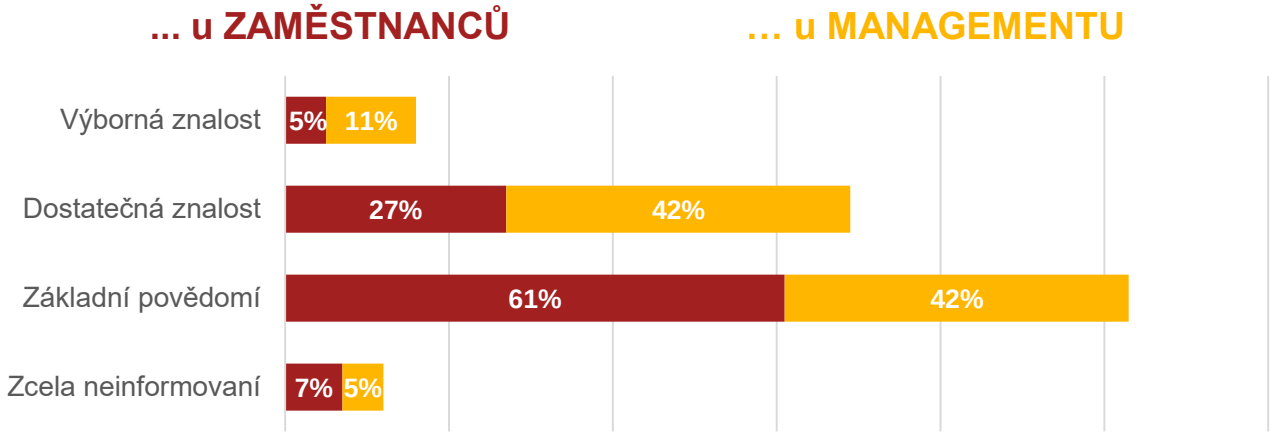
Cyber Arena

- Simulace rozvoje digitálních služeb ve vaší společnosti v kontextu probíhajících kybernetických útoků.

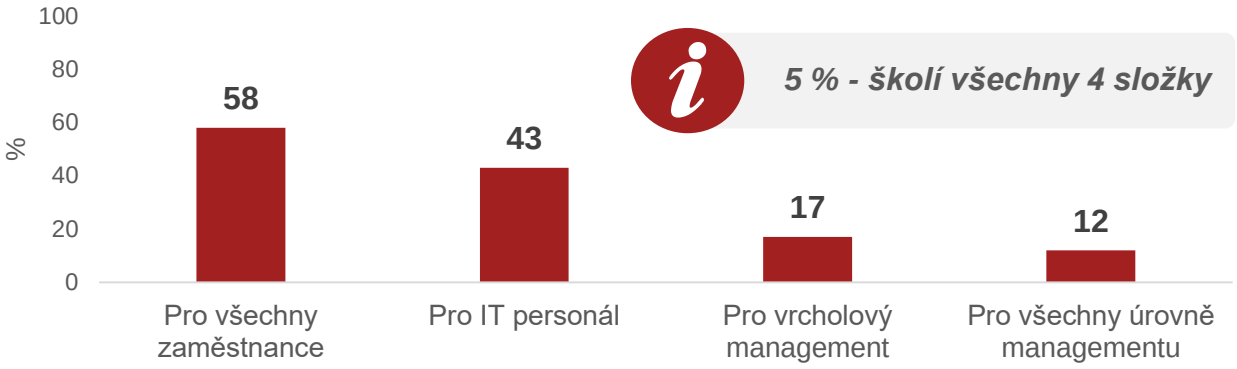
CYBERGYM® EUROPE

- Praktický týmový výcvik postavený na skutečných scénářích kybernetické války.
- Simulace prostředí konkrétní organizace, ověření schopností týmu v detekci a reakci na incident.
- Vysoce specializovaný výcvik na míru zakončený závěrečnou zprávou, doporučení pro implementaci v praxi.

Jak byste ohodnotili úroveň informovanosti vaší organizace o kyberbezpečnosti a možných hrozbách...



Pro koho jsou školení v oblasti kyberbezpečnosti ve vaší organizaci vykonávány?



Další zajímavá čísla

97 % - školí alespoň jednu složku

72 % - neškolí žádný management

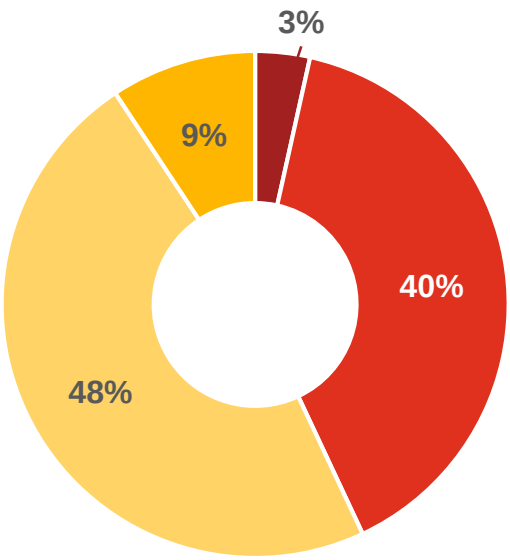
19 % - školí pouze IT personál

3 % - neškolí nic

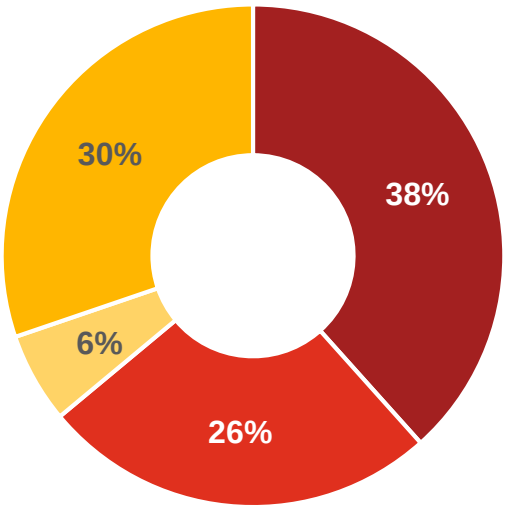
Zajímavým zjištěním, které se opakuje napříč průzkumem, je, že účastníci obecně považují management za lépe informovaný o specifikách kyberbezpečnosti. Dle odpovědí má dostatečné znalosti nadpoloviční většina managerů, zaměstnanců však pouze necelá třetina. Paradoxně je management skupinou, která je nejméně proškolená. Tuto disproporci lze částečně vysvětlit tím, že management je mnohem častěji zapojen do rozhodovacích procesů týkajících se řízení rizik, čímž jeho povědomí roste.

Vztah mezi úrovní informovanosti managementu/ zaměstnanců a uskutečněnými školeními

MANAGEMENT



ZAMĚSTNANCI



Uvedené grafy ukazují vzájemné vazby úrovně informovanosti a četnosti školení u zaměstnanců a managementu. Do těchto výsledků nebyl započítán vrcholový management, který tvoří specifickou skupinu.

Z výsledků je patrné, že téměř **v polovině organizací neprobíhají školení managementu, ovšem management je považován za dostatečně informovaný**. Ale v dalších 40 % organizací, kde také školení neprobíhají, management za dostatečně informovaný považován není.

Dále platí, že pokud už management proškolený je, tak školení splní požadovaný cíl.

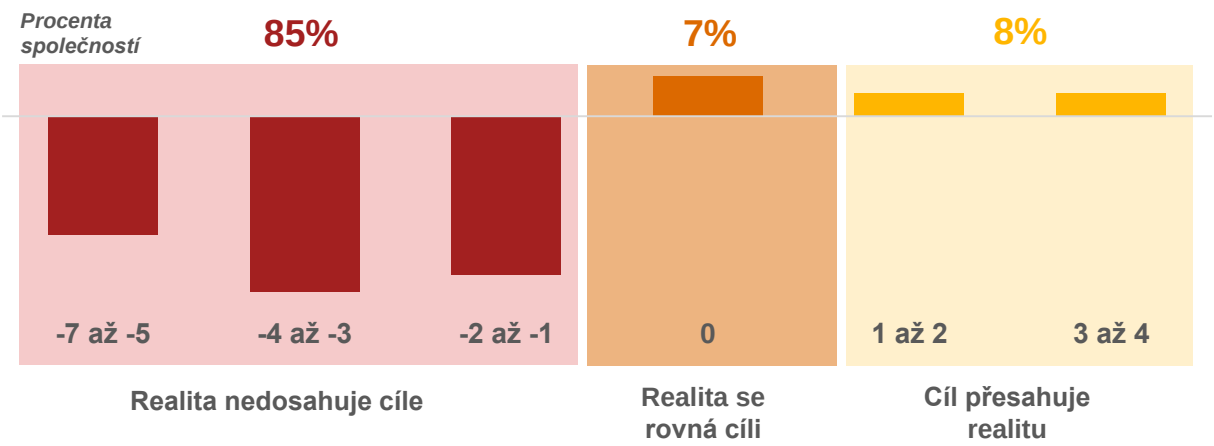
- Nedostatečná informovanost, probíhají školení
- Nedostatečná informovanost, neprobíhají školení
- Dostatečná informovanost, neprobíhají školení
- Dostatečná informovanost, probíhají školení

V případě zaměstnanců je situace odlišná. Pouze přibližně třetina organizací hodnotila svoje zaměstnance jako dostatečně informované. Alarmující však je, že i když se zaměstnanci účastní školení, tak je vzdělávacích cílů dosaženo pouze v necelé polovině případů. V situaci, kdy **zaměstnanci nejsou dostatečně informovaní, přestože se školení účastní, se nachází 38 % organizací**.

Jaký je váš cíl a realita v dodržování předpisů v oblasti kyberbezpečnosti vašimi zaměstnanci?

Hodnotící škála u této otázky byla od 1 do 10, přičemž 10 je nejlepší možné. Do sloupců se zápornými hodnotami se zařadily společnosti, kde realita v dodržování předpisů nedosahuje cílů společnosti. I když se tato otázka zaměřovala na subjektivní vnímání respondentů, výsledek šetření není příliš optimistický. **Pouze 15 % společností** uvedlo, že dodržování pravidel kyberbezpečnosti je **v souladu s očekáváními** nebo je lehce překonává.

Rozdíl mezi realitou a cílem (agregované skupiny)



Hodnoty na horizontální ose grafu znázorňují **rozdíl mezi hodnotami**, které jednotlivé společnosti uváděly jako **realitu a své cíle** na škále od 1 do 10.

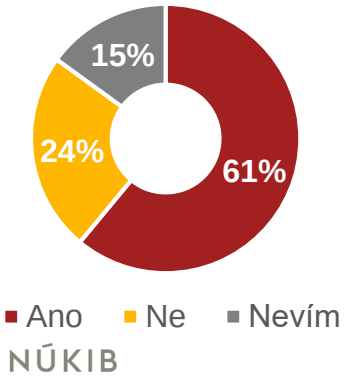
Ze zprůměrovaných dat pro cíle společností a realitu, kde hodnota 10 značí ideální stav, vyplývá, že se obecně **nedaří plnit cíle** v dodržování předpisů v oblasti kyberbezpečnosti a realita značně zaostává za očekáváním.

Cíle
7,95

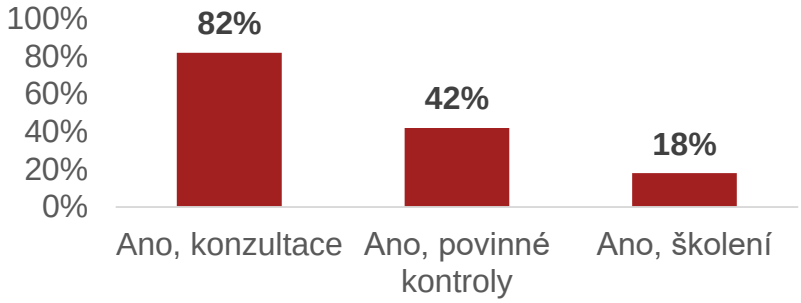
Průměrné hodnoty

Realita
5,23

Spolupracujete v oblasti kyberbezpečnosti s Národním úřadem pro kybernetickou a informační bezpečnost?



Pokud ano:



NÚKIB

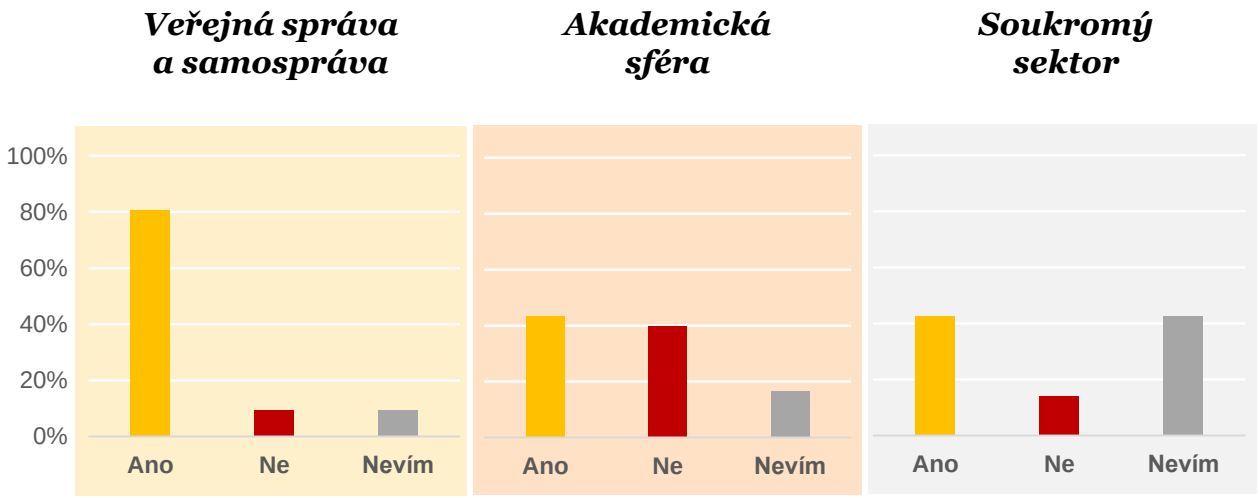
Národní úřad pro kybernetickou a informační bezpečnost

Nadpoloviční část organizací zapojených do průzkumu spolupracuje s NÚKIB. Mimořádně zajímavým zjištěním je, že velká část spolupráce se odehrává na dobrovolné bázi v rámci aktivit, které NÚKIB poskytuje pro zapojené organizace.

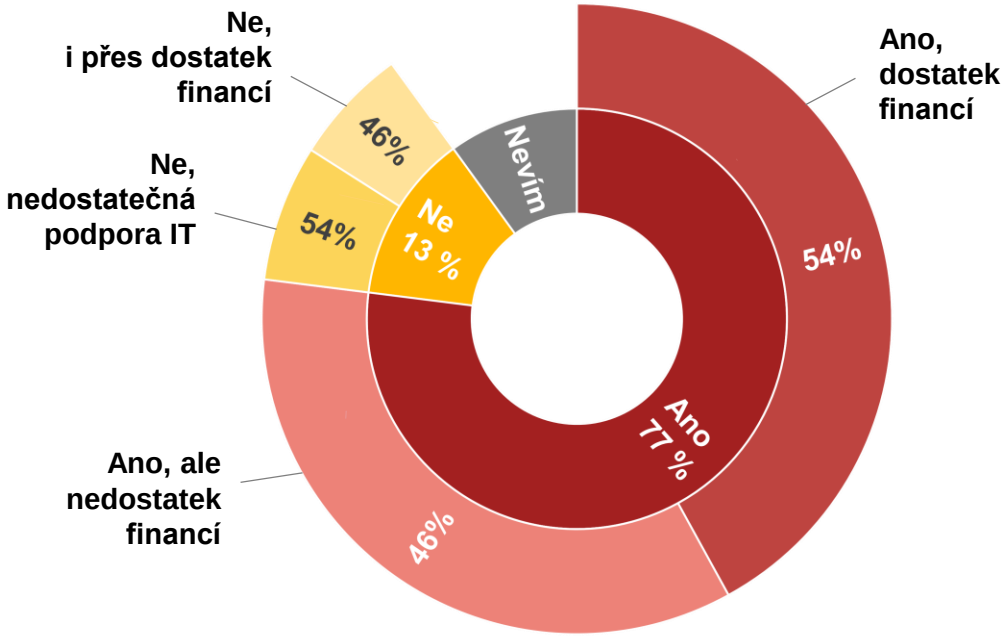
Novinky v oblasti řízení kybernetické bezpečnosti v posledním období:

- **Směrnice NIS – Směrnice evropského parlamentu a rady (EU) 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii** ze dne 6. července 2016.
- **Novela zákona o informačních systémech veřejné správy** (dříve zákon č. 365/2000 Sb., nově zákon č. 104/2017 Sb.) s účinností od 1. července 2017 **mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti.** Novinky, které tato novela přináší, jsou:
  - Zavedení **provozovatele** jako nové kategorie povinného subjektu.
  - Zpřísnění pokut za porušení povinností.
- **Novela zákona o kybernetické bezpečnosti** (dříve zákon č. 181/2014 Sb., nově zákon č. 105/2017 Sb.) s účinností od 1. srpna 2017 **implementuje změny ze směrnice NIS.** Novinky, které tato novela přináší, jsou:
  - Zavedení nových kategorií povinných subjektů – **provozovatelé základních služeb a poskytovatelé digitálních služeb.**
  - Zajištění **bezpečnosti kritických informačních systémů.**
  - Náležitosti, které musí být součástí smluv s **poskytovateli služeb cloud computing.**
  - **Likvidace** dat, provozních údajů a informací včetně jejich kopií.
  - **Informační povinnost.**
- **Vyhláška o kritériích pro určení provozovatele základní služby** (č. 437/2017 Sb.)
  - Úprava odvětvových a dopadových kritérií.
  - Pro vymezení významnosti dopadu narušení základní služby na zabezpečení společenských nebo ekonomických činností.
- **Připravuje se:**
  - **Vyhláška o kybernetické bezpečnosti** (aktuálně vyhláška č. 316/2014 Sb.)
    - Novelizace v závislosti na novele zákona o kybernetické bezpečnosti.
    - Bezpečnostní opatření, kybernetické bezpečnostní incidenty, reaktivní opatření.

Spolupráce s Národním úřadem pro kybernetickou a informační bezpečnost v rámci jednotlivých sektorů?



Vnímáte podporu ze strany vedení vaší organizace v oblasti kyberbezpečnosti?



Máte povědomí, jaké typy bezpečnostních incidentů se ve vaší organizaci objevují?

Pokud ano, které?

Nový trend: Internet věcí a ransomware

Chytré domácí spotřebiče, mobily, kamery, bezpečnostní systémy a další vzájemně komunikující zařízení jsou stále populárnější, a tím se stávají zajímavými cíli pro kyberzločince.

V roce 2016 byl zdokumentován případ, kdy útočníci převzali kontrolu nad chytrými termostaty. Ty byly přenastaveny tak, aby zvýšily teplotu v budově až na 99°C. V případě nezaplacení výkupného by útočníci mohli nechat dům vyhořet. Dalším příkladem tohoto typu útoku je ovládnutí elektronického systému zámků v rakouském hotelu. Hosté se nemohli dostat do pokojů a byla požadována peněžní částka za jejich odblokování.

Jaké významné trendy v oblasti kyberbezpečnosti vnímáte v roce 2017 a jaké očekáváte v roce 2018?

Útoky na cloudové služby

Ohromné množství aplikací má přístup ke cloudovým systémům. I mobilní zařízení, na kterém se kompromitovaná aplikace nachází, může být potenciálním nástrojem pro vzdálený útok na veřejný i privátní cloud, případně na připojené firemní sítě.

Zneužití kryptoměn

Útočníci podvodnými aktivitami získali prostřednictvím virtuálních měn nové možnosti příjmu. Kyberzločinci je v roce 2017 nejčastěji využívali pro platby za opětovné zpřístupnění zašifrovaných souborů pomocí ransomwaru. Využití kryptoměn pro zločinné účely bude i nadále pokračovat. K tomu se přidají další trendy spojené s kryptoměnami, např. zvýšení počtu hackerských útoků na burzy kryptoměn.

Manipulace finančních trhů

Existují organizované zločinecké skupiny, které se snaží získat informace o finančních výsledcích společností před jejich zveřejněním, případně informace o spojení firem před oznámením veřejnosti. Cílem zneužití těchto informací útočníky je manipulace akciových trhů nebo insider trading.

Ochrana se buduje v síti, nikoli kolem ní

Globální útoky WannaCry a Nyetya se dokázaly z jednoho zařízení rozšířit do celé sítě. Dnes se do sítí v každé organizaci připojuje mnoho typů zařízení. Chránit je nutné nejen počítače či mobilní zařízení, ale i další zařízení jako jsou tiskárny. Bezpečnostní prvky se musejí stát integrální součástí interní sítě, protože právě tam útoky probíhají. Budovat zabezpečení na perimetru sítě už dnes nestačí.

Děkujeme

Děkujeme vám, že jste si našli čas a zodpověděli naše otázky na Letním SOIRÉE s biografem, které se konalo 7. 9. 2017.

Doufáme, že jsou pro vás výsledky našeho průzkumu přínosem a věříme, že vám poslouží ke zvyšování bezpečnostního povědomí ve vašich organizacích.

V případě jakýchkoli nejasností a otázek se na nás, prosím, bez váhání obraťte.

Neváhejte nás kontaktovat

Tomáš Kuča

Tomáš je partnerem oddělení PwC pro řízení rizik, které je zodpovědné za Českou republiku a Slovensko, vede tým odborníků se zaměřením na IT audit, technologické poradenství, IT bezpečnost a compliance.

tomas.kuca(at)pwc.com

Michal Wojnar

Michal je spoluzakladatelem Business Continuity Fóra v České republice, odborníkem na kybernetickou bezpečnost a krizové řízení s více než 9 lety zkušeností v oblasti IT.

michal.wojnar(at)pwc.com

Michal Čábela

Michal má více než 9 let zkušeností v oblasti informačních technologií, vývoji SW a IT konzultací, které jsou zaměřené především na oblast kyberbezpečnosti.

michal.cabela(at)pwc.com

Karin Gubalová

Karin se zabývá informační bezpečností více než 20 let, specializuje se na bezpečnostní governance, strategii, risk management a bezpečnostní vzdělávaní.

karin.gubalova(at)pwc.com

Prostor pro vaše poznámky

StaySecure

Vaše měsíční dávka kybernetické bezpečnosti

O StaySecure

Zajištění kybernetické bezpečnosti je naší prioritou. Proto našim přátelům a dobrým klientům nabízíme zjednodušení šíření osvěty mezi vlastními zaměstnanci.

StaySecure je měsíčník, který pravidelně a jednoduchou formou seznámí Vaše zaměstnance s klíčovými oblastmi kybernetické bezpečnosti.

StaySecure je tu pro Vás zdarma.

Jak to funguje?

1. Napište nám, že **máte zájem** na daniel.hofman@pwc.com
2. Každý **první den v měsíci dostanete** do emailu nové vydání StaySecure v neutrálním designu
3. Design **můžete upravit** jakkoliv chcete
4. StaySecure **vytisknete** a vyvěsíte na nástěnky, v kuchyňkách, pošlete emailem, zveřejníte na intranetu…
5. Vaši zaměstnanci jsou zase o něco chytřejší a Vy máte **méně práce**

…jednoduché, že? ☺

Co získáte?

- Srozumitelně vysvětlené základy kybernetické bezpečnosti
- Splnění regulatorních požadavků na zvyšování povědomí o kybernetické bezpečnosti
- Více uvědomělé zaměstnance i vedení společnosti
- Pomoc se šířením osvěty od profesionálů v oboru
- Úsporu finančních prostředků – StaySecure je zdarma

46% IT bezpečnostních incidentů je způsobeno zaměstnanci

pwc

www.pwc.cz/ras