info CONSULT | SYSTÉMY OCHRANY DÁT

Bezpečnostné povedomie zamestnanca a jeho vplyv na IT bezpečnosť firmy

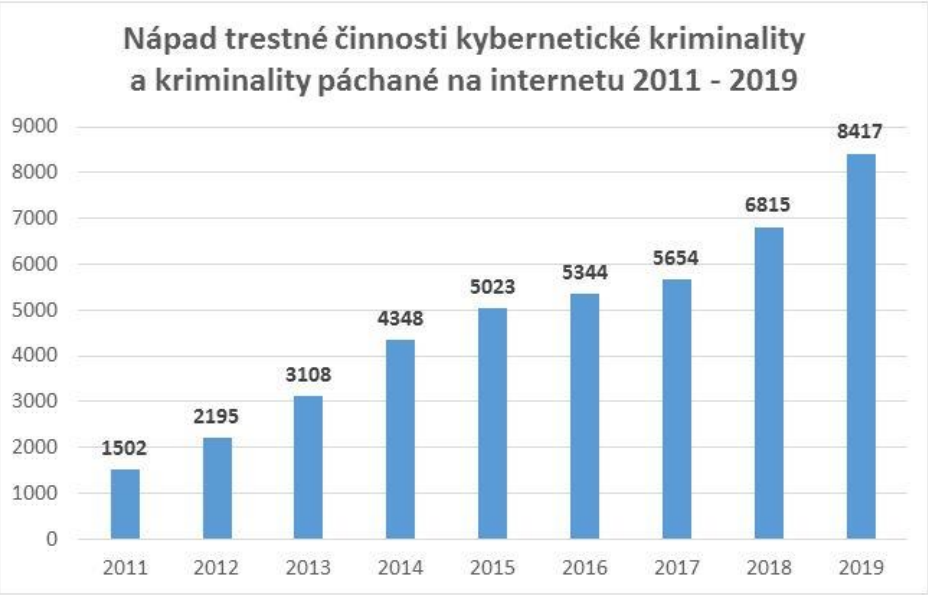
Jaroslav Oster

…pár myšlienok na úvod

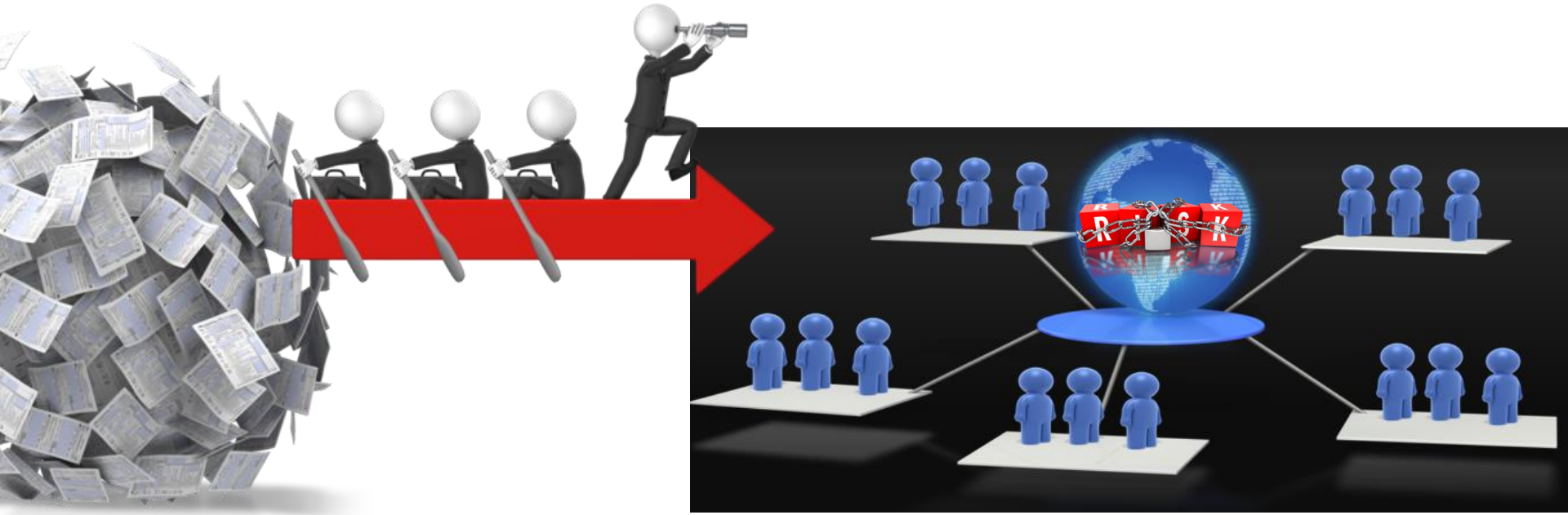
Neformálna diskusia v rámci pracovných debát Asociácie kybernetickej bezpečnosti (AKB):

AKB Asociácia kybernetickej bezpečnosti

„Odklonenie zdrojov (pozornosť, čas, financie)
od prirodzených problémov (deravá aplikácia, zanedbaná infraštruktúra, poddimenzovaný alebo nedostatočne vzdelaný security staff)
ku compliance problému (poďme vyrobiť formálny štít)“



..keď sa manažment rozhodne pre ISMS



…ako to môže dopadnúť

… najčastejšie

Časté formy úniku

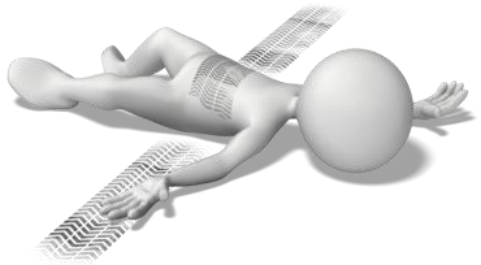
- chyby obsluhy
  - neznalosť, arogancia, cielené obchádzanie opatrení
  - necvičený personál
  - zámerné konanie (útok voči organizácii) – **sociálna manipulácia**
- organizačné nedostatky/problémy riadenia
- nezabezpečený prevádzkový perimeter na všetkých úrovniach
- chyby IS
  - chyby vývoja IS – funkčné chyby
  - chyby implementácie IS
  - zlé konfigurácie OS/ SW
- a široké spektrum ďalších frekventovaných chýb

Mýtus: Máme špičkové IT oddelenie

Technické opatrenia vyriešia všetko

„my máme nasadené špičkové bezpečnostné riešenia, všetko je vyriešené, naši ľudia sú uvedomelí“

- technické riešenie pokrýva obvykle konkrétne riziko/ skupinu rizík
- nerieši organizačné problémy
- nerieši otázky **bezpečnostného povedomia** používateľov IS, ich návykov a už vôbec nie koncepčného a efektívneho vzdelávania



môžeme snáď predpokladať, že autonómne autá dáme do rúk (ne)vodičom bez vodičského oprávnenia?

scenár manipulátora má nepísané zákonitosti

MYSTIFIKÁCIA ROLE

- sleduje cieľ
- volí manipulačnú metódu
- navodenie situácie

SCENÁR
- deklarácia autority
- deklarácia oprávnenosti
- navodenie problematickej situácie
- ponuka riešenia

REAKCIA

- stotožňuje sa s požiadavkou
- plní požiadavku (návrh) útočníka
- znáša dôsledky (škoda)

...sociálna manipulácia = riziko najvyššie

- neistota napr.časový stres, netrpezlivosť
- neznalosť
- nesústredenosť
- povrchnosť
- manipulovateľnosť
- dôvera v technické vymoženosti
- anonymita pri komunikácií telefónom
- dôverčivosť, láskavosť, ľútosť
- ochota (snaha) pomáhať
- obava z dôsledkov postoja, chovania alebo zodpovednosti
- snaha vyhýbať sa konfliktným situáciám
- zvedavosť (otvorenie prílohy, použitie nájdeného USB)
- snaha o zlepšenie aktuálneho sociálneho statusu

METÓDY SOCIÁLNEJ MANIPULÁCIE

Phishing
NEW: Spear phishing
Ransomware
Podvody s faktúrami
Ponuky na finančnú spoluprácu
Ponuky na dedičstvo
Pharming

E-MAIL

Prezváňanie z audiotextových čísiel
Falšovanie identity osoby – pokyn od nadriadeného

TELEFONICKY

Vstup na pracovisko - mystifikácia oprávnenosti
servisný technik
údržba
Pokus o prístup k citlivým dátam
Získavanie prevádzkových informácií

OSOBNE

PODHODENIE USB KĽÚČA

phishing – vysoká škola manipulačných techník

Re: Objednávka NO-2019-12000192

MRK Contract s.r.o. 8:12
Príjemca: Recipients

1.2
2_image_p...

Objednav...
ZIP - 859 kB

Prílohy: 2 (885 kB)

Dobré ráno a šťastný nový rok!

Teraz, keď sú vaše kancelárie po sviatkoch späť,

Ocenili by sme rýchlu reakciu na náš e-mail uvedený nižšie.

Môžete potvrdiť prijatie tejto objednávky?

S Pozdravom,

Martina Miškayová

MRK Contract s.r.o.
Stara Prievozska 2
821 09 Bratislava
Tel.: +421 2 53 60 71 92
Fax: +421 2 53 63 74 18
Mobil: +421 915 877 563
E-mail: martina-miskayova@mrk.sk
Web: www.mrk.sk

Before printing think about your responsibility & commitment with the **Environment!**

PRIVILEGE AND CONFIDENTIALITY NOTICE: The information contained in this e-mail communication and any attached documentation may be privileged, confidential or otherwise protected from disclosure and is intended only for the use of the designated recipient(s). If the reader or recipient of this

dar

vlada@bsnet.sk 3:14
Príjemca: Recipients

Dostali ste dar vo výške 2 400 000,00 EUR, vyhral som americkú lotériu v hodnote 40 miliónov U.S dolárov v Amerike a rozhodol som sa venovat cast z toho piatim šťastným ludom a charitatívnym domom na pamiatku mojej neskorej manželky, ktorá zomrela na rakovinu. Pre viac informácií ma kontaktujte na:
infotomcristt@gmail.com

phishing – vysoká škola manipulačných techník

st 18.12.2019 12:15

PRIMA BANKA <edison546@edison546.com>

Oznámenie o sviatočnej sezóne

Komu undisclosed-recipients:

Vážený zákazník

je tu nový vývoj, ktorý vás chráni pred vianočnými útokmi z podvodníkov online.

Požiadali sme vás, aby ste sa zúčastnili tejto najnovšej ponuky od Prima Bank a zabránili zneužitiu vášho účtu.

navštívte: https://ib.primabanka.sk/ib/default.aspx

Toto je bezpečná správa a želáme vám všetkým vopred Veselé Vianoce.

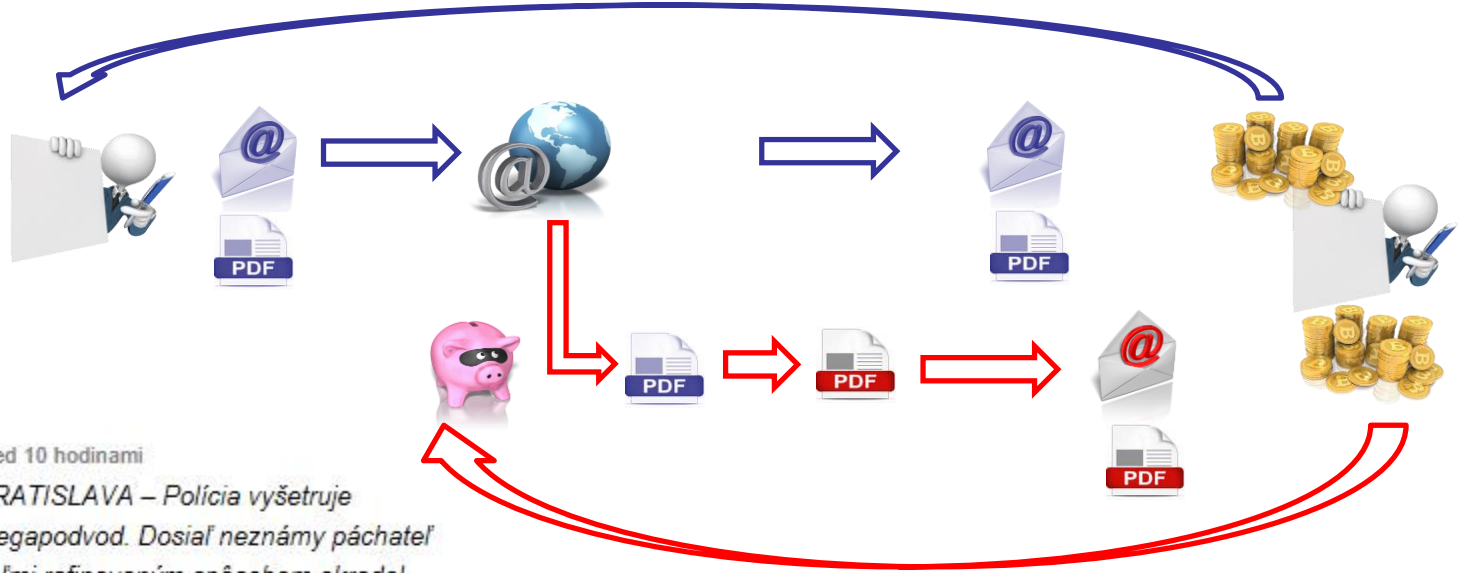
úprimne

Prima banka

... manipulačné techniky v realite

Podvody s faktúrou....len trochu upravené

2016-2017.....2018, 2019



Ilustračné foto
Zdroj: Getty Images

pred 10 hodinami

BRATISLAVA – Polícia vyšetruje megapodvod. Dosiaľ neznámy páchateľ veľmi rafinovaným spôsobom okradol spoločnosť o 167 524 eur. Muži zákona i Ministerstvo vnútra SR (MV SR) v tejto súvislosti upozorňujú verejnosť na podvodné prevody peňazí. Poškodená firma prišla o danú sumu len jedným kliknutím.

LUDSKY FAKTOR

…aktuálny a diskutovaný príklad…nie je jediný

Výpadek začal ve 02:17 na chirurgické ambulanci, kde se zpomalovaly počítače, a v 02:50 již nebyly IT systémy funkční po celé nemocnici. Virus překonal bránu firewall a dva aktuální antivirové systémy.

„Napadl většinu serverů a pracovních stanic, jichž je 300. V současné době je významně omezen provoz nemocnice. Nelze spustit žádný laboratorní ani žádný jiný přístroj včetně počítačové sítě. V nemocnici zasedl operativně krizový štáb pro řešení nastalé situace," uvedl ředitel nemocnice Roman Mrva. V ordinacích podle něj nelze provést vyšetření, ambulantní specialisté přeobjednávají pacienty na jiné termíny.

Ransomvér Ryuk 8/2018

Šíri sa prostredníctvom dôkladne pripravených e-mailových správ, ktoré prevažne cielia na podniky a organizácie.

...ako je zamestanec „oklamaný“

útočník zasiela
e-mail s prílohou

pripojenie downloaderu
– URL hostingu ransomware

nakazenie počítača
- stiahnutie ransonware

postupné zašifrovanie
súborov

zobrazenie výzvy

úhrada výpalného
útočníkovi

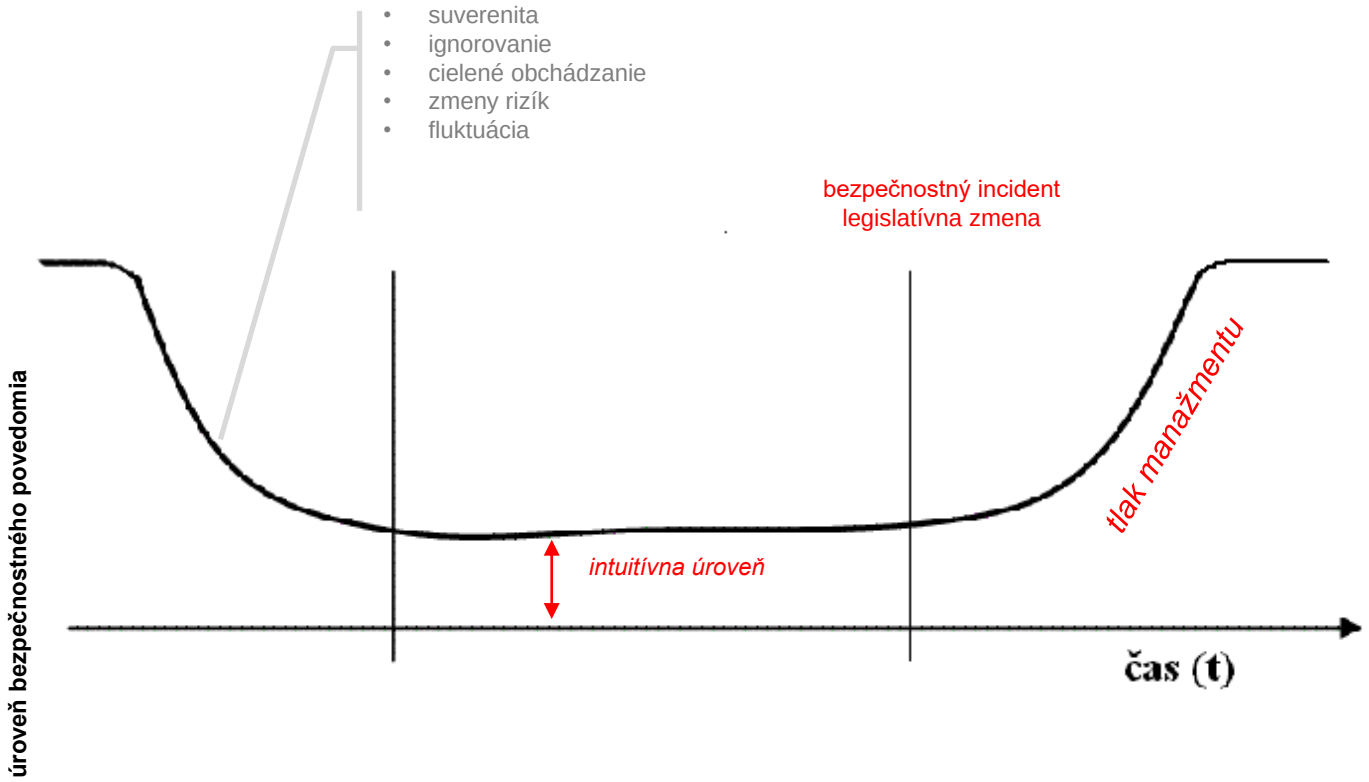
KĽÚČ ????

Zásadné omyly

Zamestanec používajúci IT ako pracovný nástroj (neIT)

- intuitívne chápanie IT bezpečnosti je mýtus
- viera v samoštúdium v mimopracovnom čase nefunguje
- poučenie OO vo formáte podľa 122ky nie je zvyšovaním bezpečnostného povedomia

Budovanie bezpečnostného povedomia



Legislatívno - normatívne argumenty

Legislatíva, norma	Definícia požiadavky
GDPR (18/2018) +158/2018 Vyhláška o postupe pri posudzovaní vplyvu na ochranu osobných údajov	**§ 49 Vnútropodnikové pravidlá** 1 - n) primeraná odborná príprava fyzických osôb, ktoré majú stály alebo pravidelný prístup k osobným údajom, v oblasti ochrany osobných údajov.
ZoKB 69/2018 Z.z. vyhláška 362/2018 Z.z. Vyhláška, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení	**Bezpečnostné opatrenia pre oblasť podľa § 20 ods. 3 písm. c) zákona** Personálna bezpečnosť pozostáva najmenej b) zo zavedenia plánu rozvoja bezpečnostného povedomia a vzdelávania ..... d) z hodnotenia účinnosti plánu rozvoja bezpečnostného povedomia, ... h) z vykonania poučenia o manipulácii s informáciami pre osoby, ktoré vykonávajú činnosť alebo sa oboznamujú s informáciami podľa osobitného predpisu
95/2019 Z. z. Zákon o informačných technológiách vo verejnej správe	**§ 19 Bezpečnosť informačných technológií verejnej správy v oblasti plánovania a organizácie** (3) Správca prostredníctvom výkonnej zložky systému riadenia bezpečnosti zabezpečuje f) organizáciu vzdelávacej činnosti pre oblasť bezpečnosti informačných technológií verejnej správy.
STN ISO/IEC 27001 Povedomie o informačnej bezpečnosti, vzdelávanie a školiaca činnosť	Všetci zamestnanci organizácie a v prípade, že je to potrebné, aj zmluvní partneri by mali absolvovať vhodné školenie v oblasti bezpečnostného povedomia a mali by sa im pravidelne poskytovať aktualizované verzie politík a postupov organizácie, tak ako si to vyžaduje ich pracovné zaradenie.

…formálny prístup negeneruje zodpovednosť

zmeny interných procesov

zmeny legislatívy

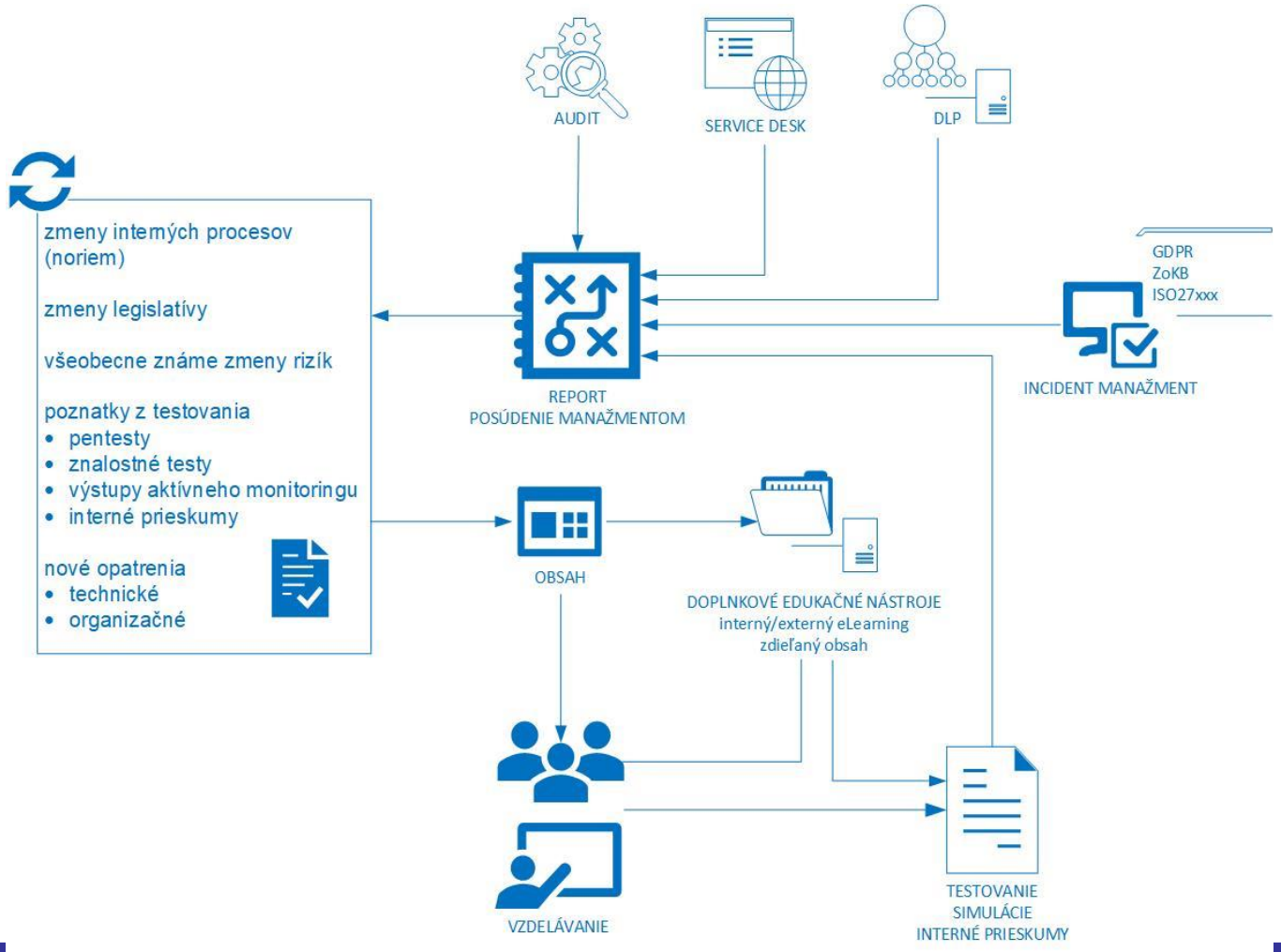
všeobecne známe zmeny rizík

poznatky z testovania
- pentesty
- znalostné testy
- výstupy aktívneho monitoringu

nové opatrenia
- technické
- organizačné

výstupy z incident manažmentu

Koncepcia = EFEKT

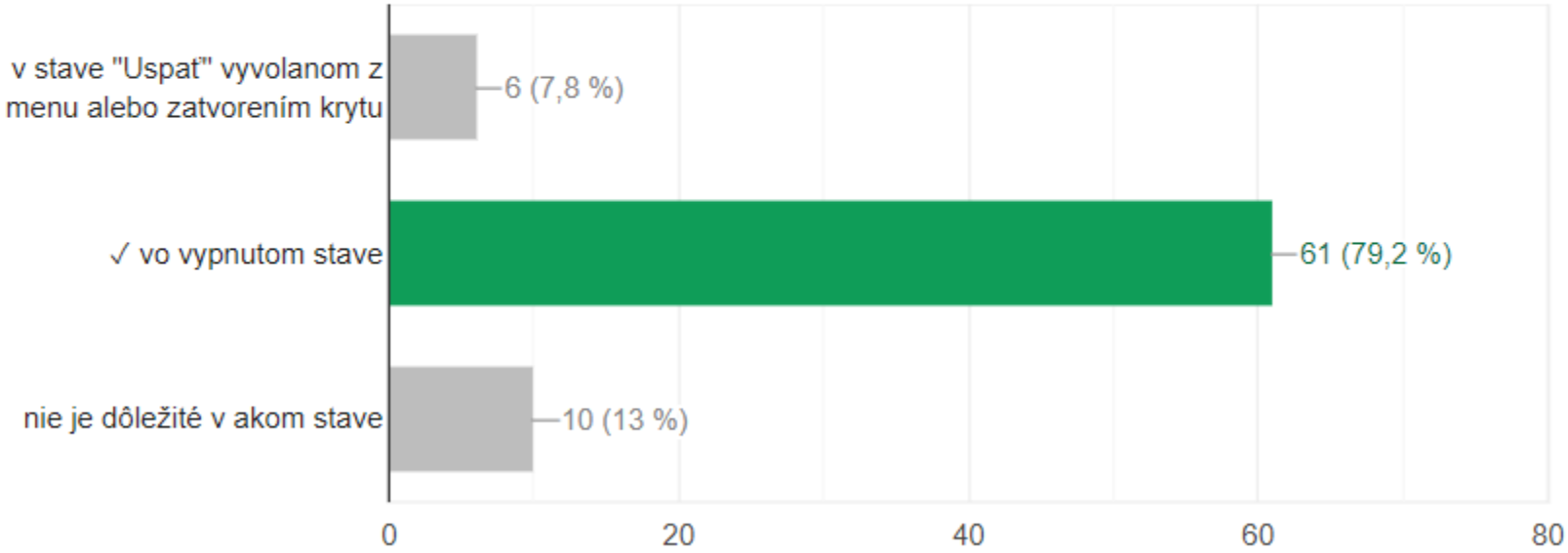


…testovanie úrovne

Riešime skutočné problémy a nie dohady

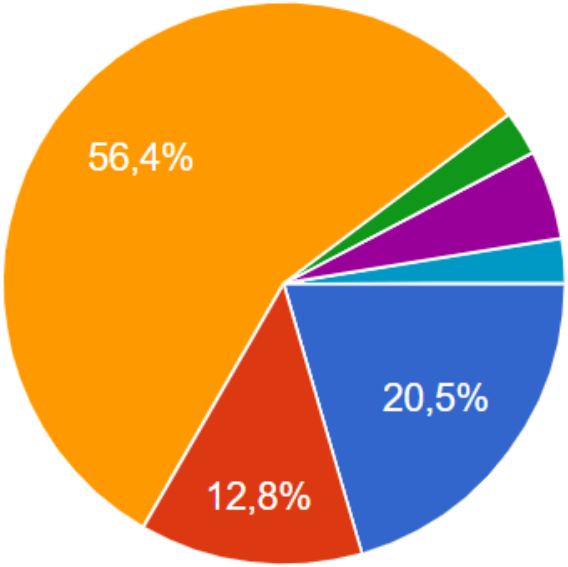
Pridelený notebook je možné prenášať mimo priestorov firmy.

61 správnych odpovedí z 77



….názory z praxe

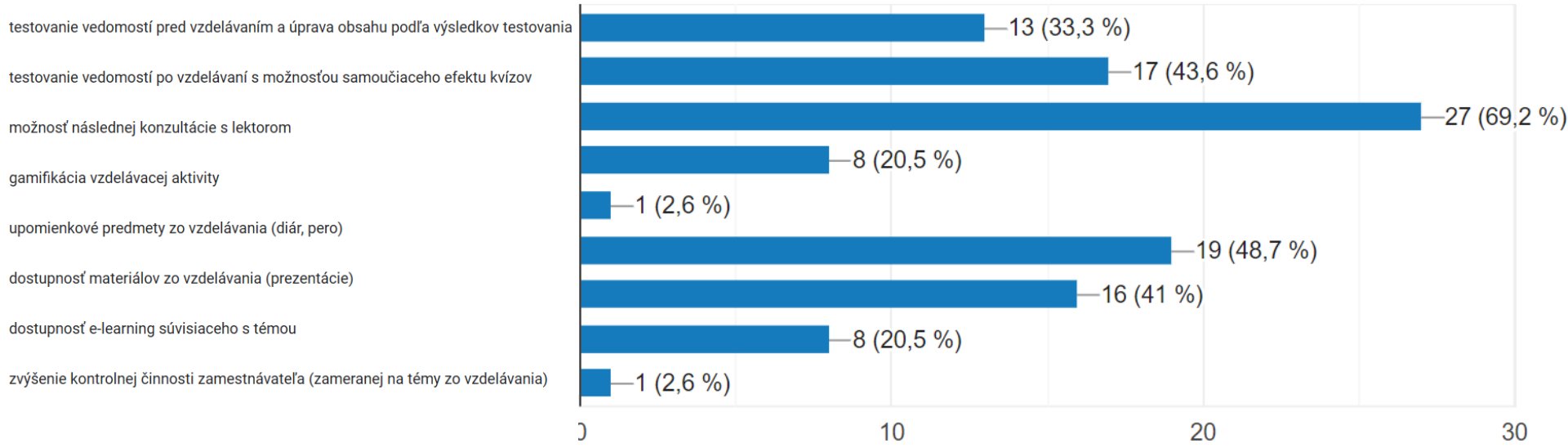
Ktorá forma vzdelávania IT security je podľa Vás najúčinnejšia?



- účasť na externých seminároch/ workshopoch organizovaných mimo pr…
- interný seminár/workshop organizovaný na pracovisku - interný lektor
- interný seminár/workshop organizovaný na pracovisku - externý lektor
- e-learningové vzdelávacie portály
- samoštúdium
- Ak sa vie školenie nastaviť dobre interne (prestávky na telefonáty a pod.), tak aj…

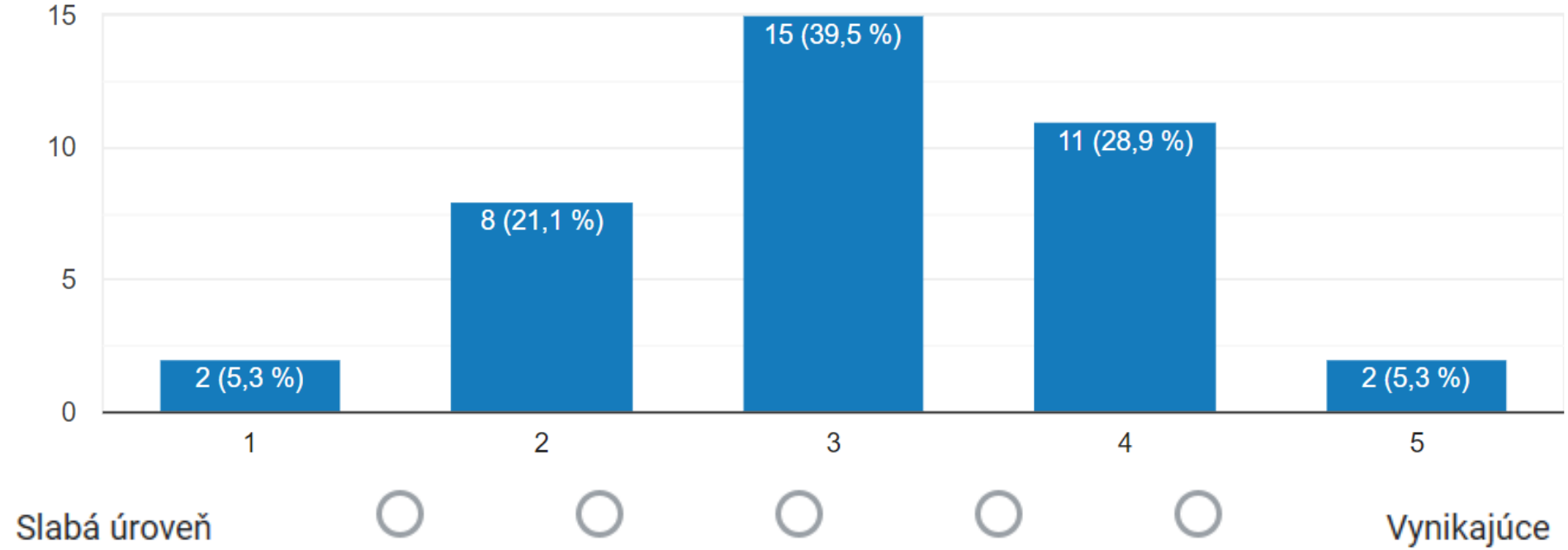
….názory z praxe

Čo podľa Vás zvyšuje efektívnosť vzdelávacích aktivít?



….názory z praxe

Ako by ste hodnotili súčasné aktivity pre zvyšovanie bezpečnostného povedomia bežných používateľov IT ktorých ste sa zúčastnili?

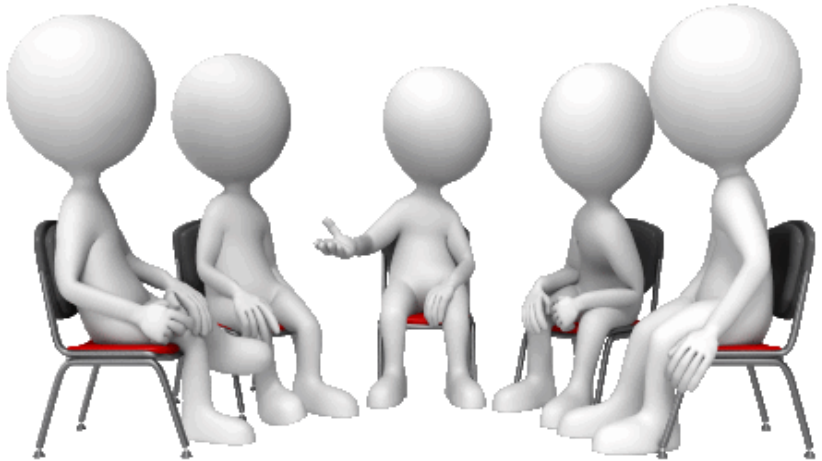


….názory z praxe – realizačné chyby

Chyby	Charakteristika
nestanovené ciele	obecný obsah bez predošlého stanovenia zámeru
nevhodný obsah alebo forma	neskúsený lektor teória odtrhnutá od praxe „všetko pre všetkých“ nevyváženosť obsahu
jednorázovosť	jednorázová aktivita vyvolaná situáciou (zmena legislatívy alebo jednorázový interný incident)
selektívnosť	zvyšovanie bezpečnostného povedomia sa týka všetkých osôb – liga výnimočných neexistuje
nesprávne nastavenie zámeru	cieľom je pochopenie, nie vyvolanie neistoty
neužitočnosť tém	témy nekorešpondujú s potrebami organizácie
bez benefitu	Postráda informačný obsah „zužitkovateľný“ aj v súkromnom živote

Rada na záver - otázky

....treba začať, sám sa tento proces nenaštartuje



...instantné, bezpracné a finálne riešenie neexistuje, zmierte sa s tým

Jaro Oster

Info consult, s.r.o.
Martina Rázusa 29
Lučenec

0905 272066

www.infoconsult.sk

oster infoconsult.sk