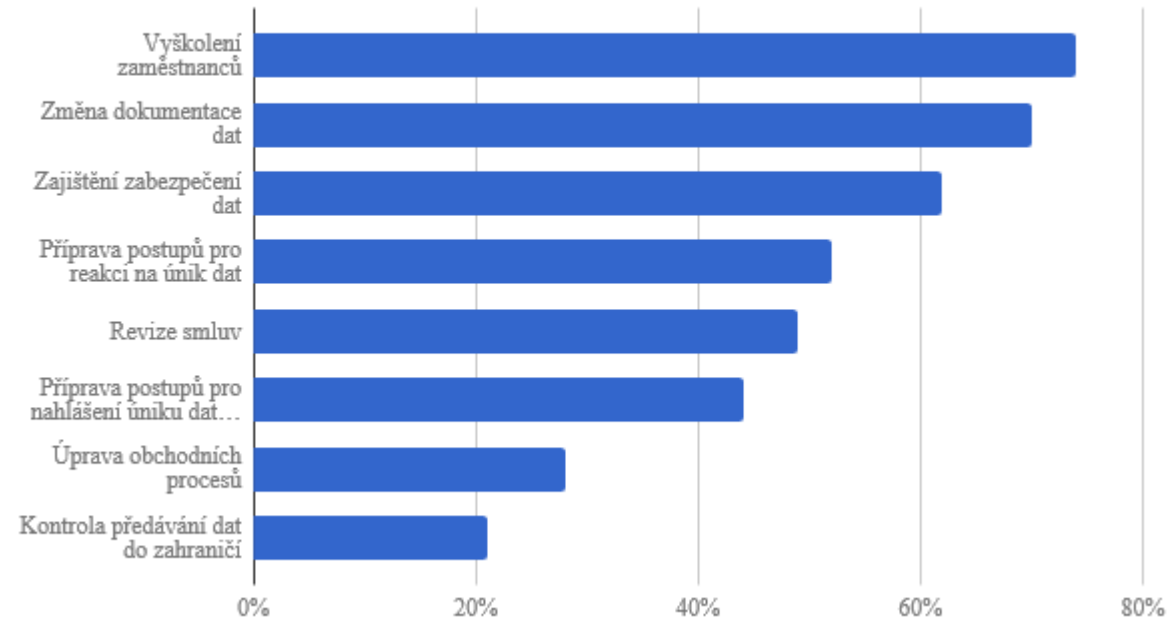


Dokážu malé a stredné organizácie postaviť GDPR na súčasnom stave?

Jaroslav Oster

Jaká opatření musí vaše firma přijmout kvůli startu GDPR?



Zdroj: <http://byznys.ihned.cz/>

prieskum IPSOS pre AMSP ČR, 6/2017

428/2002 z.z.



90/2005 z.z.



122/2013 z.z.



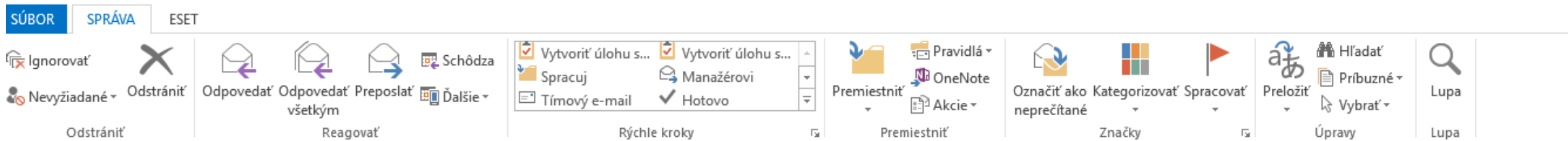
84/2014 z.z.

Stav po 15 rokoch

- nízky nárast povedomia
 - dotknuté osoby
 - oprávnené osoby
 - manažmenty prevádzkovateľov/ sprostredkovateľov
- deklaratívne naplnenie požiadaviek – segment malých/stredných organizácií
 - fiktívna dokumentácia (BP)
 - čiastočná alebo nulová implementácia bezpečnostných opatrení
- problematika poňatá ako jednorázová aktivita
 - nasadenie technologického riešenia (SW/HW)
 - jednorázové poučenie oprávnených osôb v minimalistickom rozsahu
- rad nedostatkov v riadení bezpečnosti

- prenos plného rozsahu zodpovednosti na prevádzkovateľa/sprostredkovateľa vrátane ich vzájomných vťahov
- zodpovedná osoba (DPO)
- technologické opatrenia
- **zvýšené nároky na zvyšovanie bezpečnostného povedomia**
- sprísnené a nové práva dotknutých osôb
 - zmeny súhlasu so spracovaním
 - preukaznosť slobodného a informovaného súhlasu
 - odvolanie súhlasu
 - právo byť informovaný, byť zabudnutý, právo na portabilitu
 - rozšírenie kategórií osobných údajov
 - sprísnenie spracovania OÚ detí
- **evidencia a notifikácia incidentov**





ut 9.5.2017 20:23
GULF LLC <smtp@injom.com>
[virus viaceré infiltrácie] Re: Re: Re: Invoice inquiry

Komu Recipients

Odstránili sme nadbytočné zlomy riadkov v tejto správe.

Správa Príloha bez názvu 00003.txt (125 B) Príloha bez názvu 00006.txt (125 B)

I am writing on behalf of my colleague who was on a leave

Please kindly check and confirm if the attached new order is available in your stock and please note that this order is urgently needed before the end of March, also can you accept 50% down payment for this order?

In the attached Invoice please focus of those places mark with RED

Await your urgent reply.

Best regards

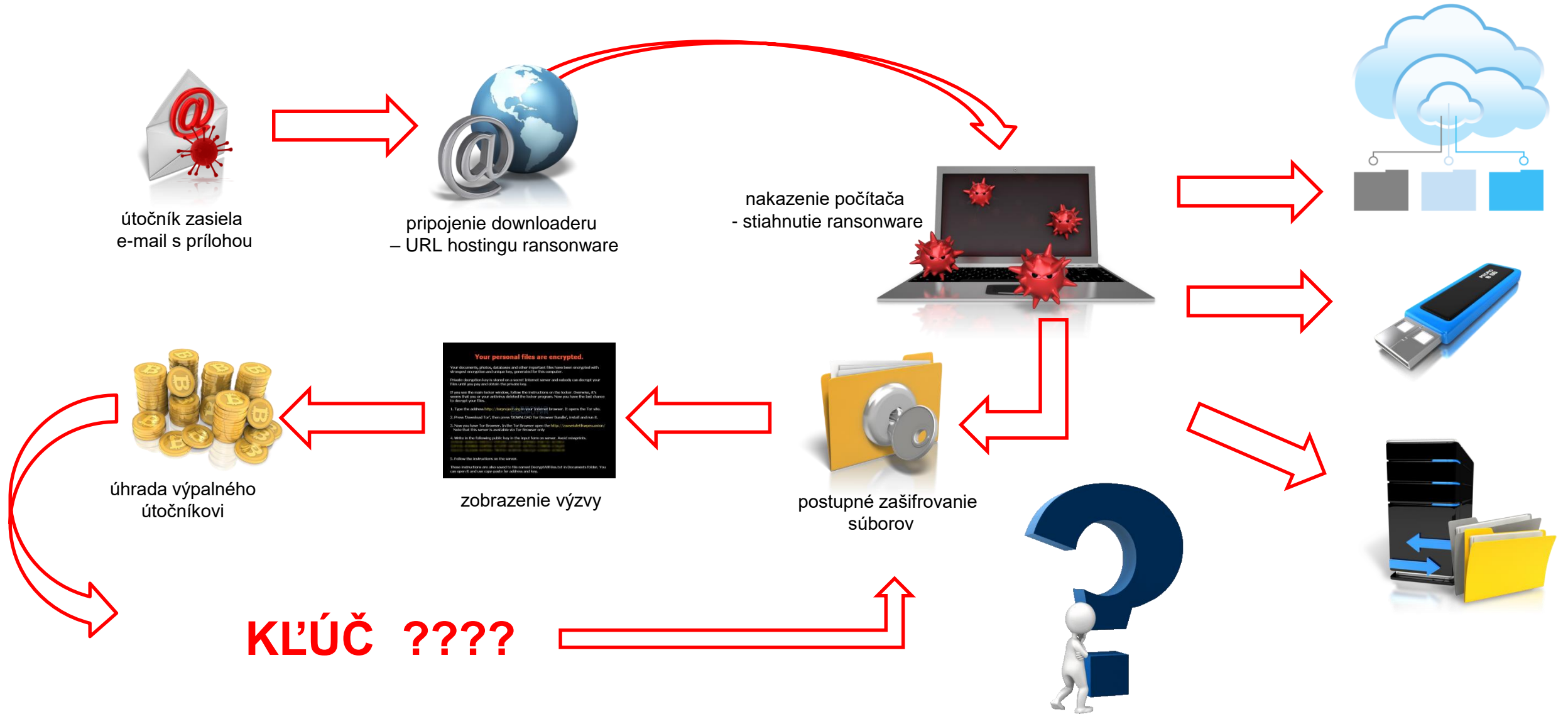
Neutromics Ukraine LLC
Kiev

.....

Sídlo (fakturační adresa):
MISTRA s.r.o., Brezina 373, 664 84 Zbraslav,
ICO: 277 23 861, DIC: CZ 277 23 861
tel.: +420 546 212 995



Kryptovírusy, ransomware – zodpovednosť používateľa





Povedomie o informačnej bezpečnosti, vzdelávanie a školiaca činnosť

Opatrenie

Všetci zamestnanci organizácie a v prípade, že je to potrebné aj zmluvní partneri a používatelia v pozícii tretích strán musia absolvovať vhodné školenie v oblasti bezpečnostného povedomia a musia im byť poskytované pravidelne aktualizované verzie politík a postupov organizácie, tak ako si to vyžaduje ich pracovné zaradenie.

Článok 47 "Závazné vnútropodnikové pravidlá"

2. V závazných vnútropodnikových pravidlách uvedených v odseku 1 sa uvedie aspoň:

n) primeraná odborná príprava personálu, ktorý má stály alebo pravidelný prístup k osobným údajom, v oblasti ochrany údajov.



Súčasné frekventované chyby



- neoznačené monitorované priestory
- porušovanie práva na súkromie zamestnancov
- nelikvidovanie záznamov po zákonnej lehote
- neexistencia bezpečnostnej dokumentácie
- nepoučenie obsluhy (oprávnené osoby)
dôsledok: porušovanie práv DO –napr.zverejnením videa
- používanie záznamov na iné účely než vymedzuje legislatíva



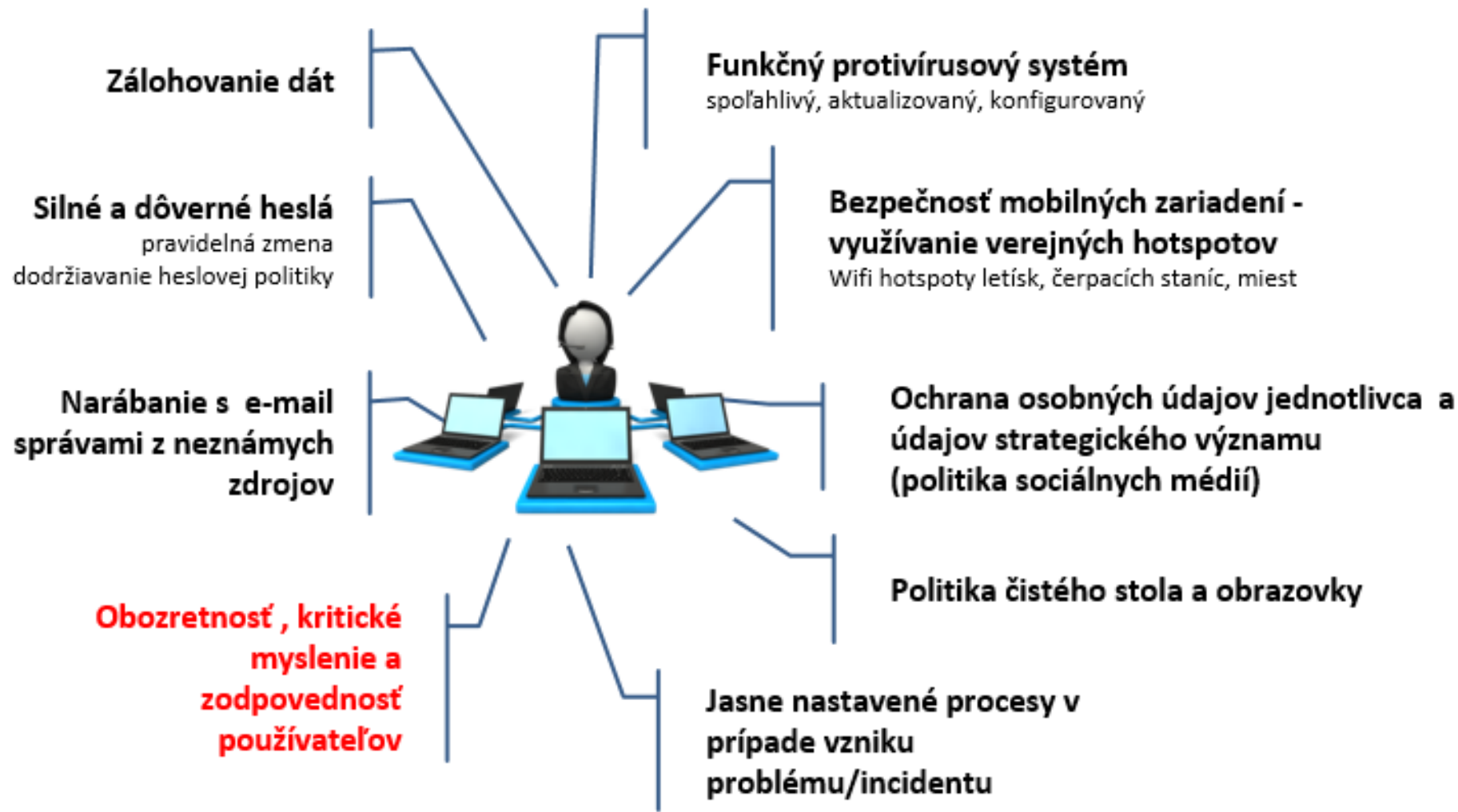
- nespracovanie BD
- BD nezodpovedá zákonu po štrukturálnej/obsahovej stránke
- BD nezodpovedá skutočnosti
 - okopírované, univerzálne (neprispôsobené) vzory projektov/smerníc*
 - nezohľadňuje skutočné riziká v danom prostredí
 - popisuje neexistujúce prostredie/stav
 - popisuje neexistujúce opatrenia
 - neprehľadné odkazy na inú dokumentáciu prevádzkovateľa
- bezpečnostné opatrenia z BD nie sú **implementované** v praxi
- oprávnené osoby nie sú informované o existencii opatrení
porušenie zákonníka práce zo strany zamestnávateľa



- určenie zodpovednostných vzťahov
 - nie je zakotvené v bezpečnostnej dokumentácii
 - nie je kompetenčne prenesené – osoby zodpovedné za jednotlivé oblasti bezpečnosti neprevzali túto zodpovednosť
 - nie je odkorešpondované smerom k používateľom
- chyby technickej implementácie opatrení
 - zlá konfigurácia
 - nepreverená funkcionálnosť (typické: neaktualizácia systémov)
 - nezdokumentovaná konfigurácia (nastavenia) – problém pri obnove
 - chýbajú recovery postupy
 - kvalita SW – často neriešiteľný problém – ak aplikačný SW nemá implementované mechanizmy

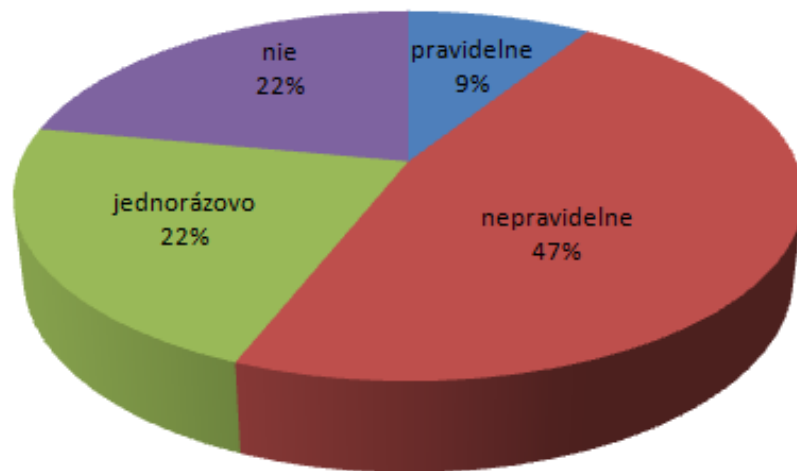


Aké máme teda základy na nadstavbu?

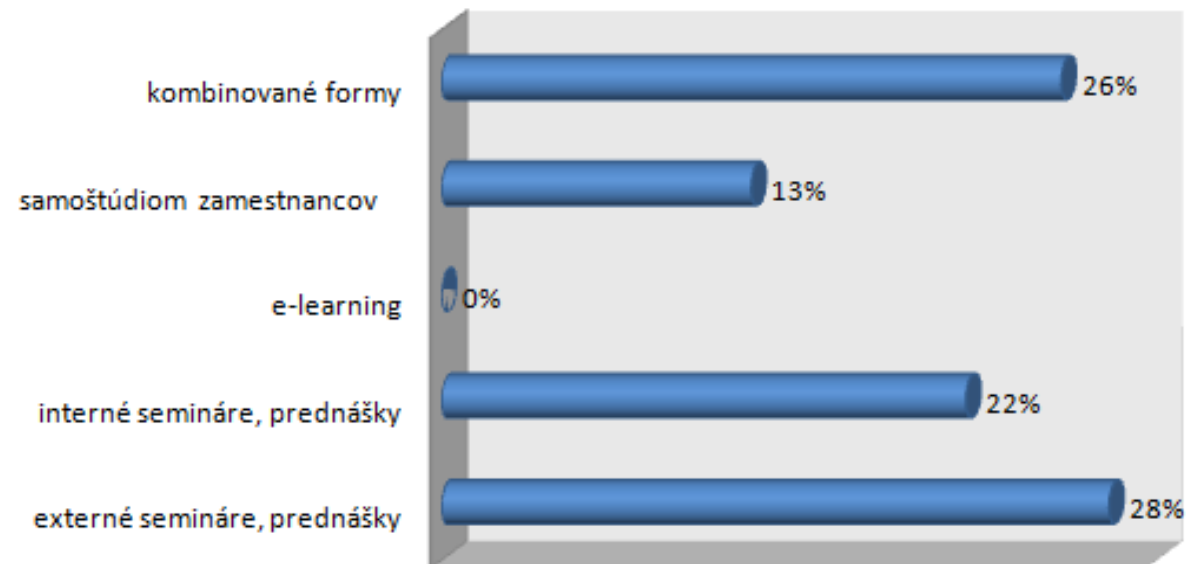


prieskum poukázal na rezervy v oblasti interného vzdelávania – **len 9% respondentov** má zavedenú pravidelnú cyklickú formu vzdelávania zamestnancov v oblasti informačnej bezpečnosti

Frekvencia



Formy vzdelávacích aktivít



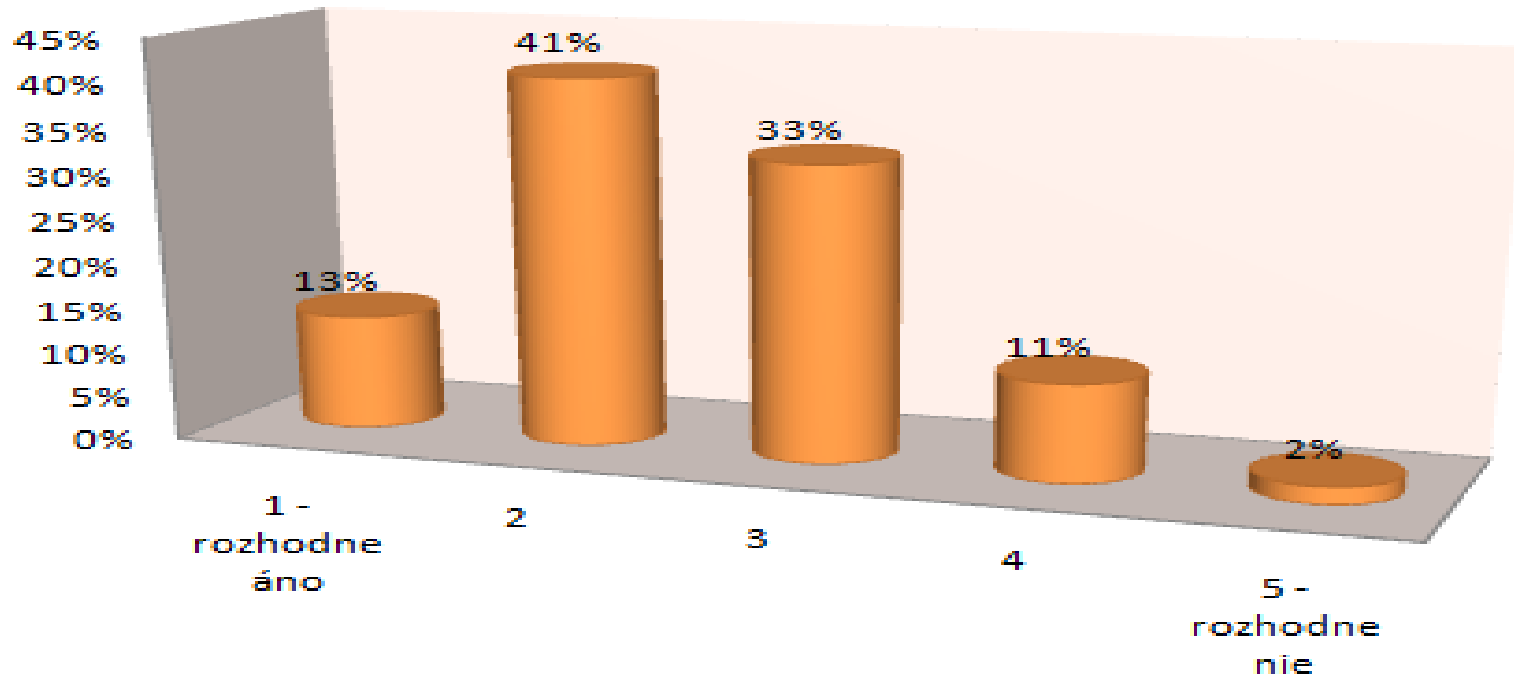
Zdroj: Prieskum Samosprávy, Info consult a Asociácia prednostov úradov miestnej samosprávy SR, 2011



Graf 16: Poučenie zamestnancov o pravidlách bezpečného používania informačných systémov

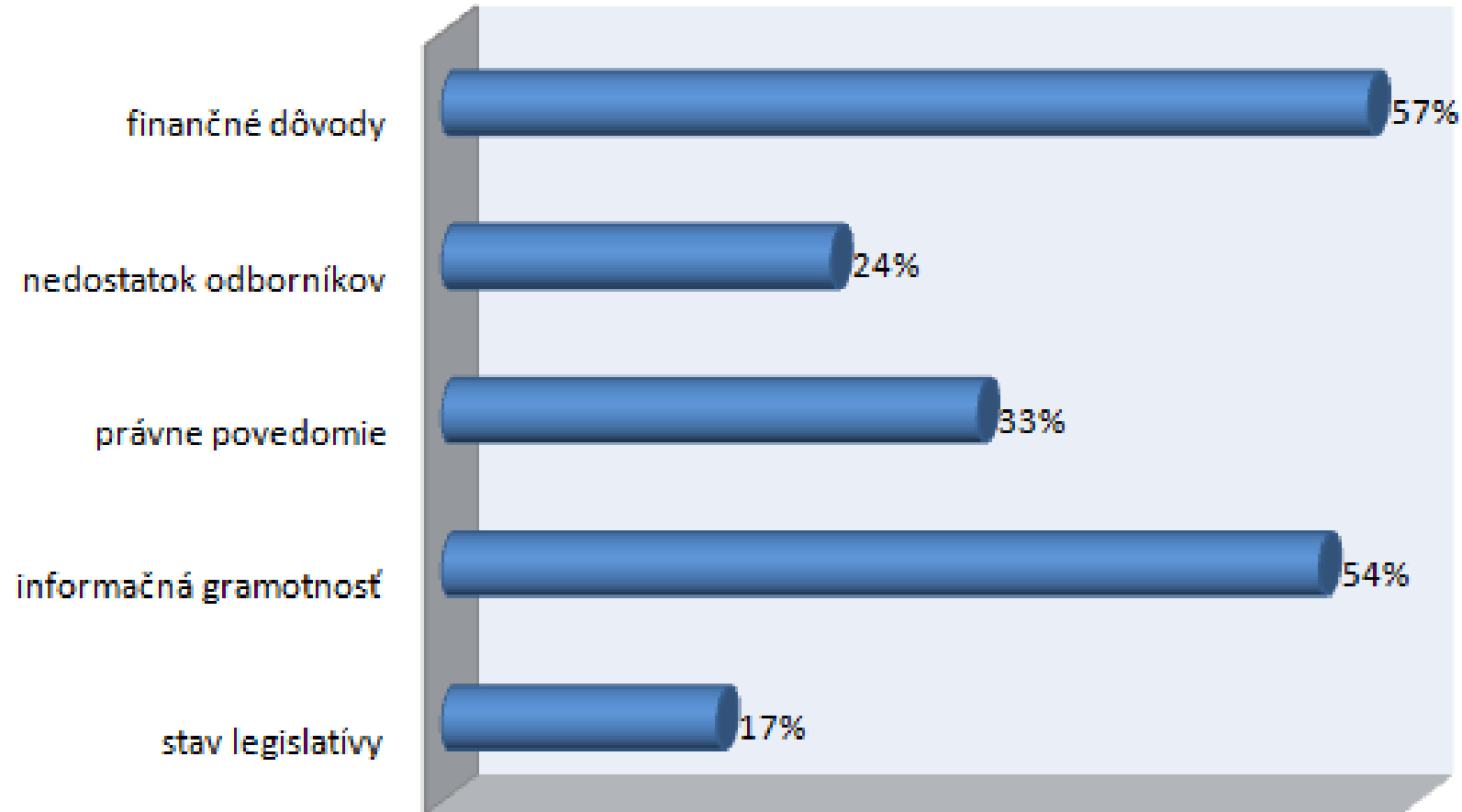
180 respondentov
Zdroj: MF SR

Na otázku „Myslíte, že Vaši zamestnanci sú dostatočne oboznámení s problematikou hesiel a ich používania?“ manažéri úradov v hodnotení 5-bodovej stupnice zhodnotili reálny stav nasledovne.



Zdroj: Prieskum Samosprávy, Info consult a Asociácia prednostov úradov miestnej samosprávy SR, 2011

V čom vidia samosprávy zásadné problémy



Zdroj: Prieskum Samosprávy, Info consult a Asociácia prednostov úradov miestnej samosprávy SR, 2011



info | SYSTÉMY
CONSULT | OCHRANY
DÁT

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

0905 272066

www.infoconsult.sk

oster@infoconsult.sk

