



Kybernetické bezpečnostné riziká v reálnej dennej praxi

Rastislav Janota
riaditeľ

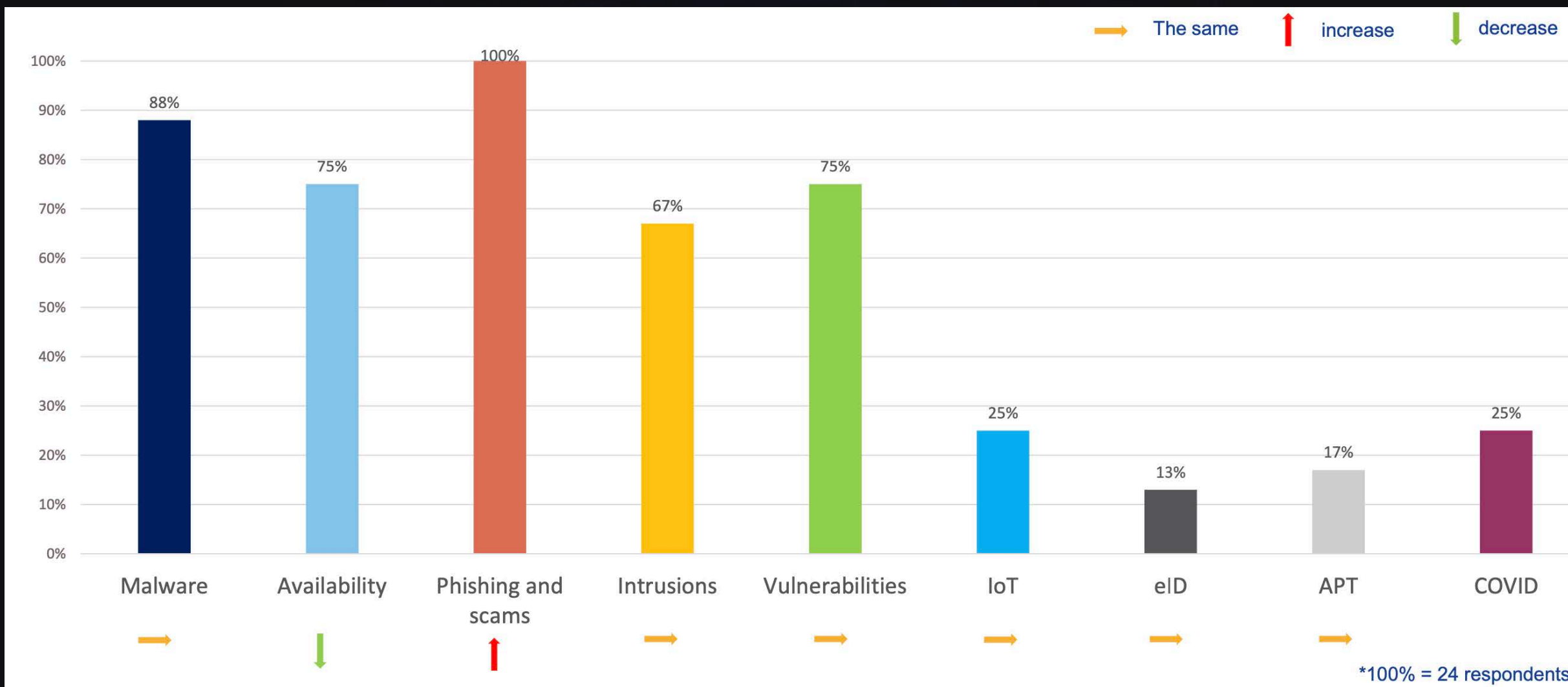


NÁRODNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI

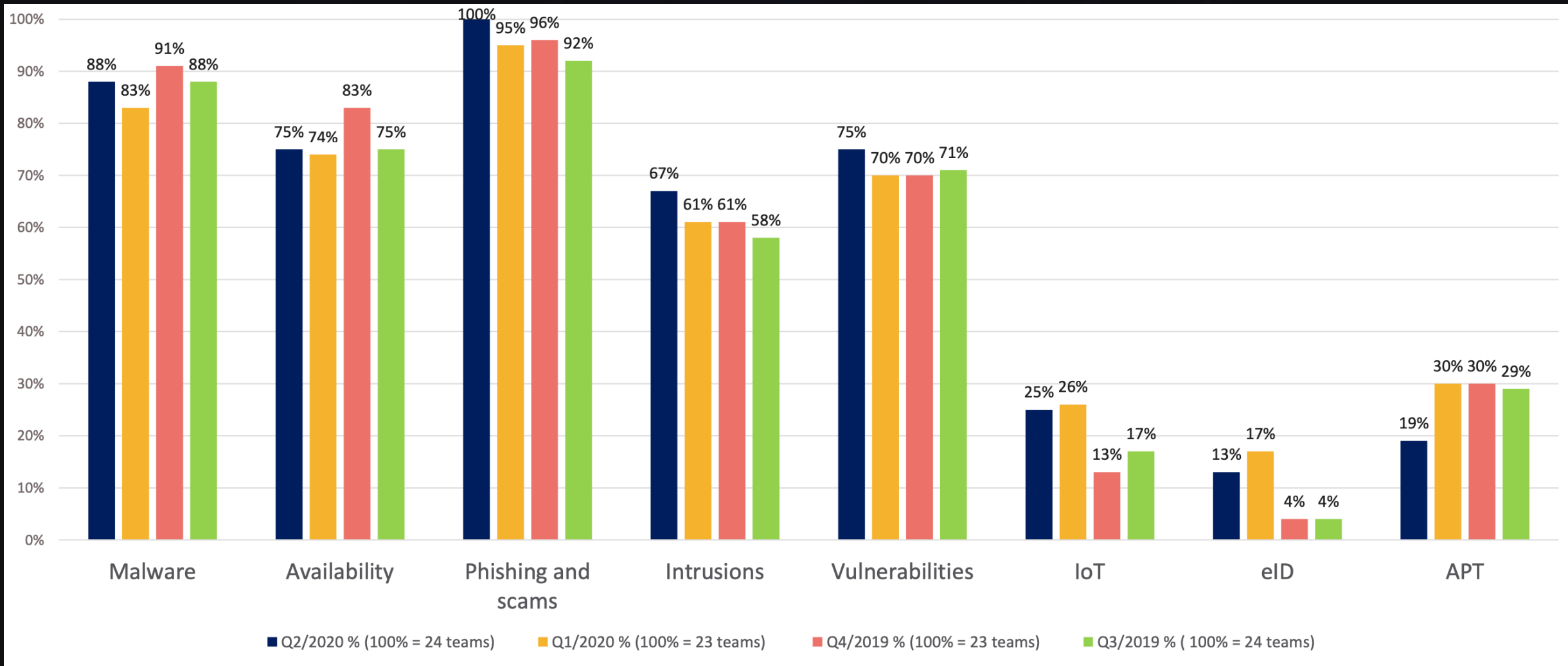


Téma kybernetickej bezpečnosti sa týka každého.

Každý je zodpovedný za svoje dáta, služby, zariadenia.



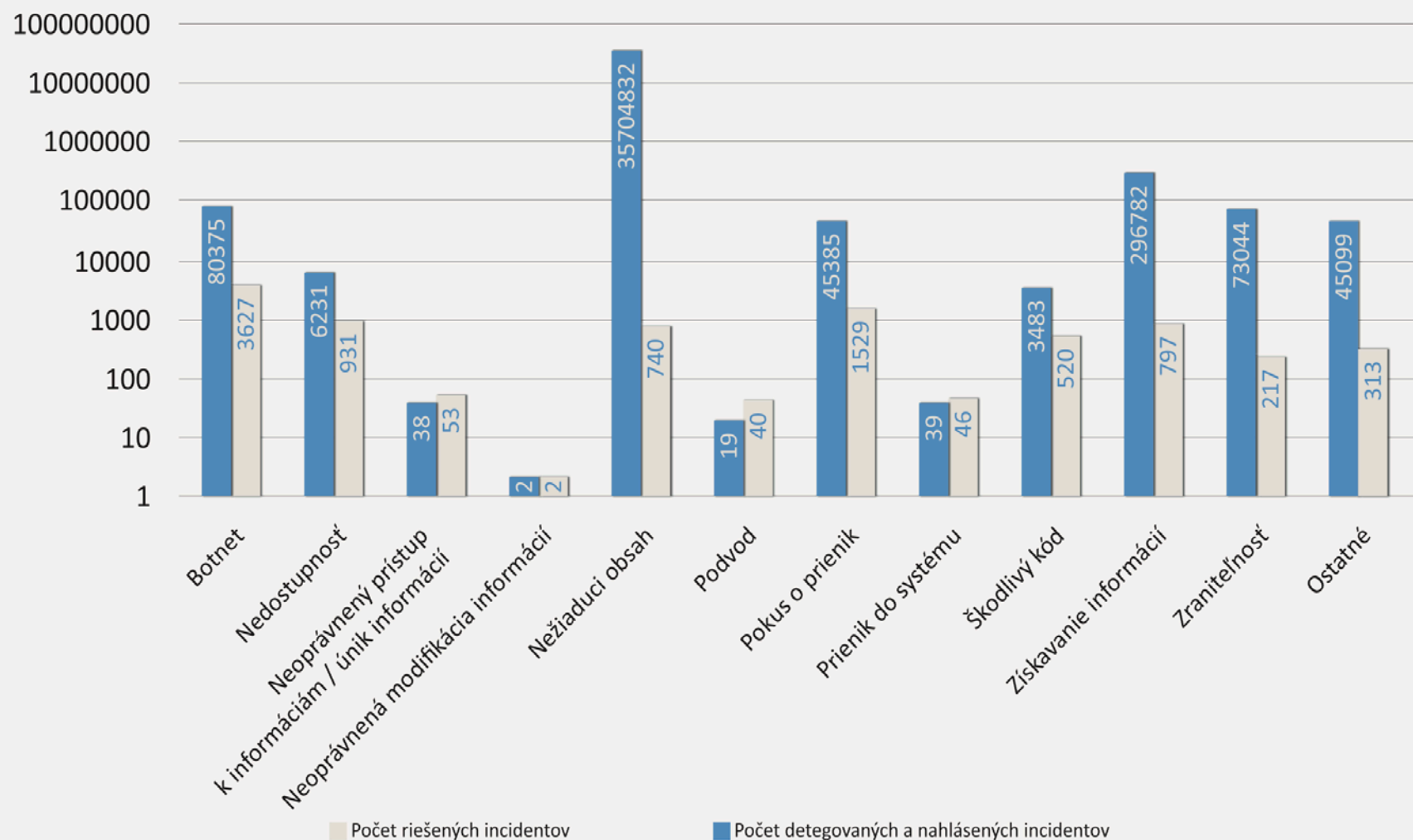
TLP: GREEN



	email	web	other	Office doc	Windows app	other
Obchod	95.2%	17.1%	0.0%	41.5%	28.2%	21.2%
Verejná správa	95.6%	15.1%	0.0%	64.4%	24.9%	16.1%
Profesionálne služby	96.9%	14.4%	0.0%	51.2%	25.0%	18.4%
Výroba	98.0%	9.0%	0.0%	37.6%	33.3%	25.7%
Informačná spoločnosť	97.7%	10.5%	0.0%	49.7%	25.3%	20.7%
Zdravotníctvo	91.1%	21.0%	0.0%	67.1%	10.0%	17.4%
Financie a poisťovníctvo	96.8%	10.3%	0.0%	74.5%	12.5%	12.6%
Školstvo	61.4%	86.1%	0.0%	26.6%	27.2%	34.2%
Ubytovanie a stravovanie	94.8%	16.7%	0.0%	56.2%	15.8%	19.0%

Zdroj: 2019 Verizon data breach investigations report

Graf č. 1: Počet detegovaných, nahlásených a riešených incidentov v roku 2019. (Zdroj: NCKB SK-CERT).



Interné riziká

- Zamestnanci – cielené ale aj náhodné škodlivé správanie

Externé riziká

- Malware, Phishing, DDoS, Ransomware, Hacking, využitie známych ale aj Zero-day zraniteľností, MitM útoky, SQL injekcie, XSS, social engineering a veľa ďalších spôsobov.

Čo je horšie?

- Obidve sú porovnateľne devastujúce
- Ale v praxi to závisí od charakteru podnikania, od dát, ktoré sú dostupné a podobne
- Je nevyhnutné v praxi riešiť riziká oboch typov

- Fakes and Deep fakes –nové aktuálne buzzwordy
- Použitie mobilných zariadení ako nových brán k firemnému prostrediu
- Ransomware je sofistikovanejší a adresnejší
- Útoky na dodávateľský reťazec budú čoraz častejšie
- DevOps urýchľuje vývoj softvéru, ale zvyšuje bezpečnostné riziká
- Využívanie honeypotov a emulovaných prostredí je na vzostupe – ale musia byť dôveryhodné
- Častejšie využívanie cloudu prináša iné incidenty – tzv cloud based incidenty, ktoré firmy typicky nevedia riešiť
- Využívanie machine learningu a AI aj zo strany útočníkov
- Návrat harwarových a firmware útokov
- Cílené útoky na power userov
- Šifrovaná komunikácia na vzostupe, zmena konceptu bezpečnostnej ochrany od perimetrovej ku end-pointom

Bezpečnostné opatrenia sa prijímajú a realizujú najmä pre oblasť

- a) organizácie kybernetickej bezpečnosti a informačnej bezpečnosti,
- b) riadenia rizík kybernetickej bezpečnosti a informačnej bezpečnosti,
- c) personálnej bezpečnosti,
- d) riadenia prístupov,
- e) riadenia kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami,
- f) bezpečnosti pri prevádzke informačných systémov a sietí,
- g) hodnotenia zraniteľností a bezpečnostné aktualizácie,
- h) ochrany proti škodlivému kódu,
- i) sieťovej a komunikačnej bezpečnosti,
- j) akvizície, vývoja a údržby informačných sietí a informačných systémov,
- k) zaznamenávania udalostí a monitorovania,
- l) fyzickej bezpečnosti a bezpečnosti prostredia,
- m) riešenia kybernetických bezpečnostných incidentov,
- n) kryptografických opatrení,
- o) kontinuity prevádzky,
- p) auditu, riadenia súladu a kontrolných činností.

Vyhláška NBÚ č. 362/2018 Z.z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení

Kde teda máme najviac problémov v reálnom svete?

Manažment

- Nevnímanie bezpečnosti
- Zlá predstava o zodpovednosti
- Neochota investovať

Bezpečnostní profesionáli

- Veľký nedostatok ľudí
- Nekvalita celkovo
- Slabé bezp. Vedomosti
- Málo vzdelávania

IT zamestnanci

- Slabá predstava o bezpečnosti
- Zvyklosti, zotrvačnosť
- Chýbajúce bezpečnostné vzdelávanie

Užívatelia

- Neochota obmedzovať sa
- Neznalosť rizík
- Slabý awareness

Governance

- Absencia kultúry riadenia rizík v organizácii
- Chýbajúce prepojenie fyzickej, personálnej a informačnej bezpečnosti
- Nedostatočná evidencia assetov, klasifikácia informácií a kategorizácia sietí a informačných systémov,
- Chýba riadenie bezpečnosti v dodávateľskom reťazci

Bezpečnostná prevádzka

- Bezpečnostné centrum s 24/7 resp podľa typu businessu (aj externe)
- Chýbajúca správa zraniteľností
- Nevyhodnocovanie logov z prevádzkovaného HW a SW
- Chýba riadenie prístupov

Chýbajúce oblasti

- Používanie neaktualizovaných SW nástrojov
- Chýbajúce plány na zálohovanie a obnovu
- Podcenené antivírus nástroje, nástroje na ochranu mail komunikácie
- Podcenenie šifrovania





NATIONAL
SECURITY
AUTHORITY



Pravdepodobne by sme mohli tento rok
vyskúšať iný prístup ku kybernetickej bezpečnosti

THANK YOU
ĎAKUJEM

rastislav.janota@nbu.gov.sk



NÁRODNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI