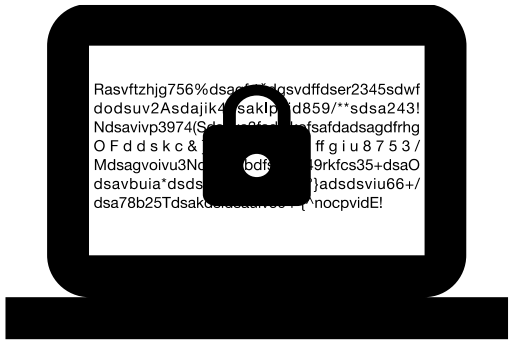
SK-CERT Threat Landscape 2021

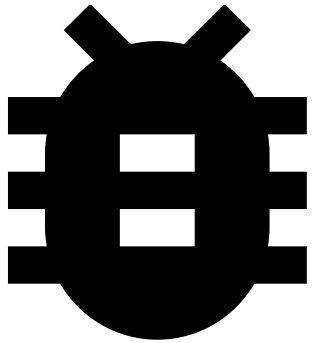
Matej Šalmík

GLOBÁLNE TRENDY



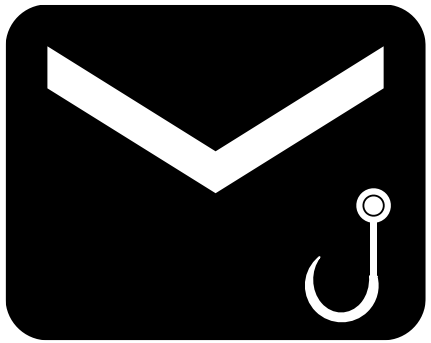
RANSOMWARE

- RaaS
- Double Extortion
- Menšia doba zotrvania v systéme obete
- Ransomvér v supply chain



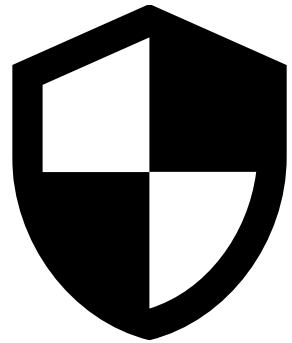
ZRANITEĽNOSTI

- Kontinuálny nárast
- Exchange zraniteľnosti
- Log4j
- Zraniteľnosti v CMS systémoch



PHISHING

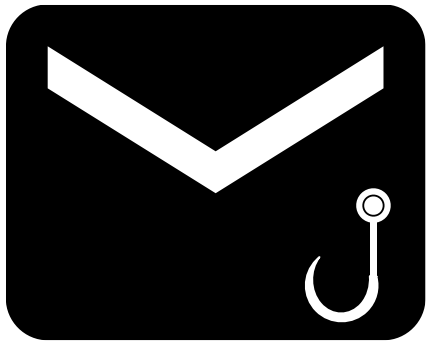
- Telefonický phishing
- Sofistikovanosť
- Blacklisty organizácií
- Smishing
- Zneužívanie kontaktných formulárov



MISC

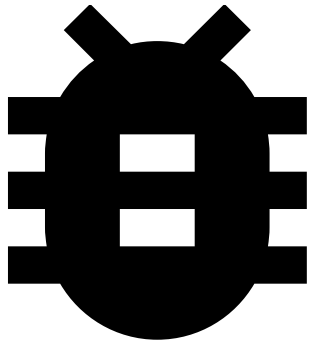
- Botnety
- Mobilný malvér
- Supply chain útoky
- Útoky na commercial
- APT útoky
- Priemyselná špionáž

SLOVENSKO – TRENDY A HROZBY



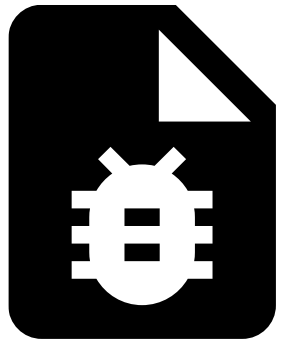
PHISHING

- Najrozšírenejší a najúčinnejší útok
- Poštové phishingy
- Získavanie bankových údajov a osobných údajov
- Chatovacie aplikácie
- Inzerentné portály



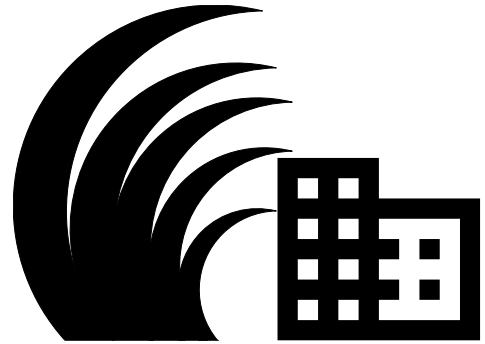
ZRANITEĽNOSTI

- Tak ako vo svete
- Exchange zraniteľnosti
- ProxyLogon, ProxyShell, ProxyNightmare
- Log4j



MALWARE

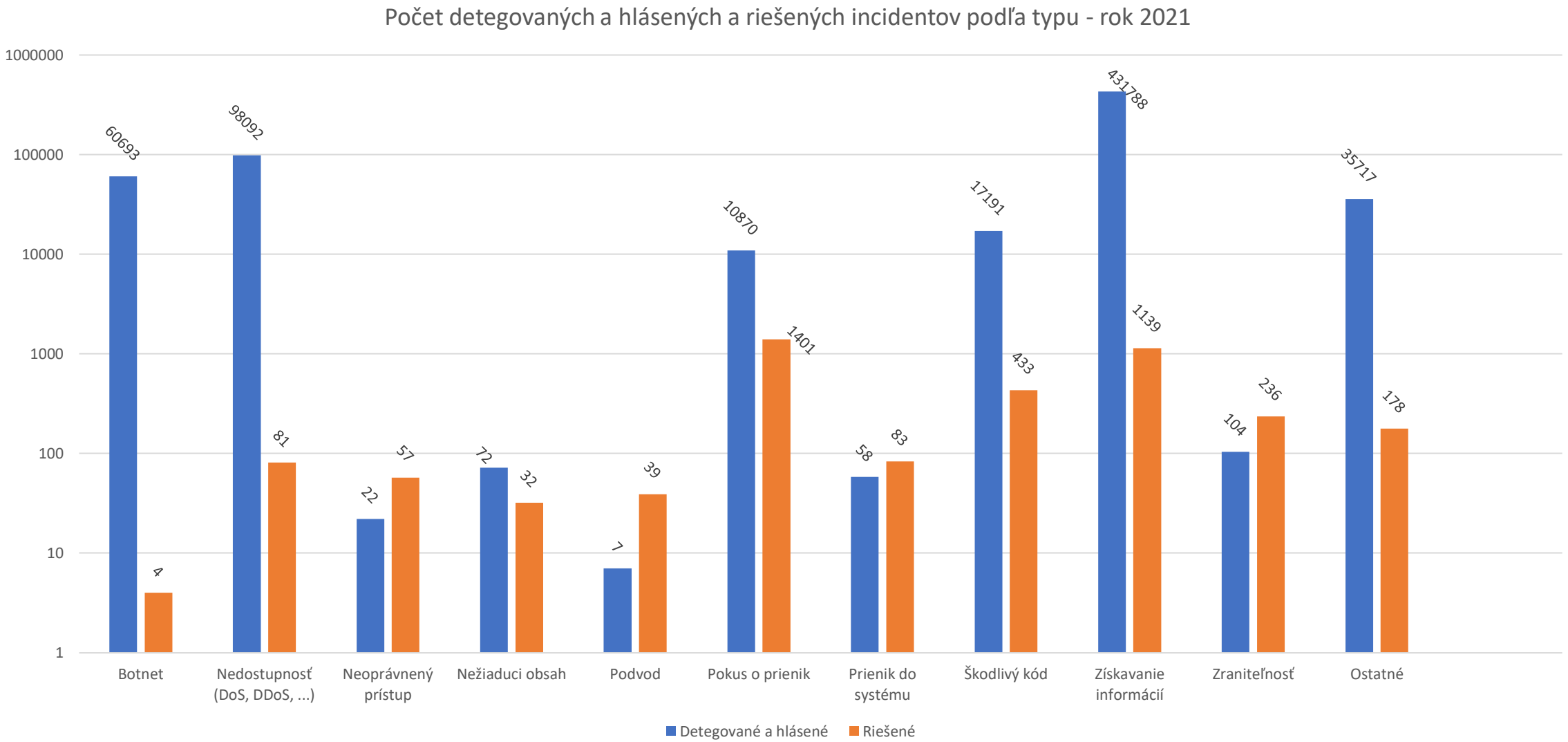
- Botnety (EMOTET, TrickBot, QuakBot, MERIS, Conficker)
- Ransomvér v samospráve
- RAT a keylogery



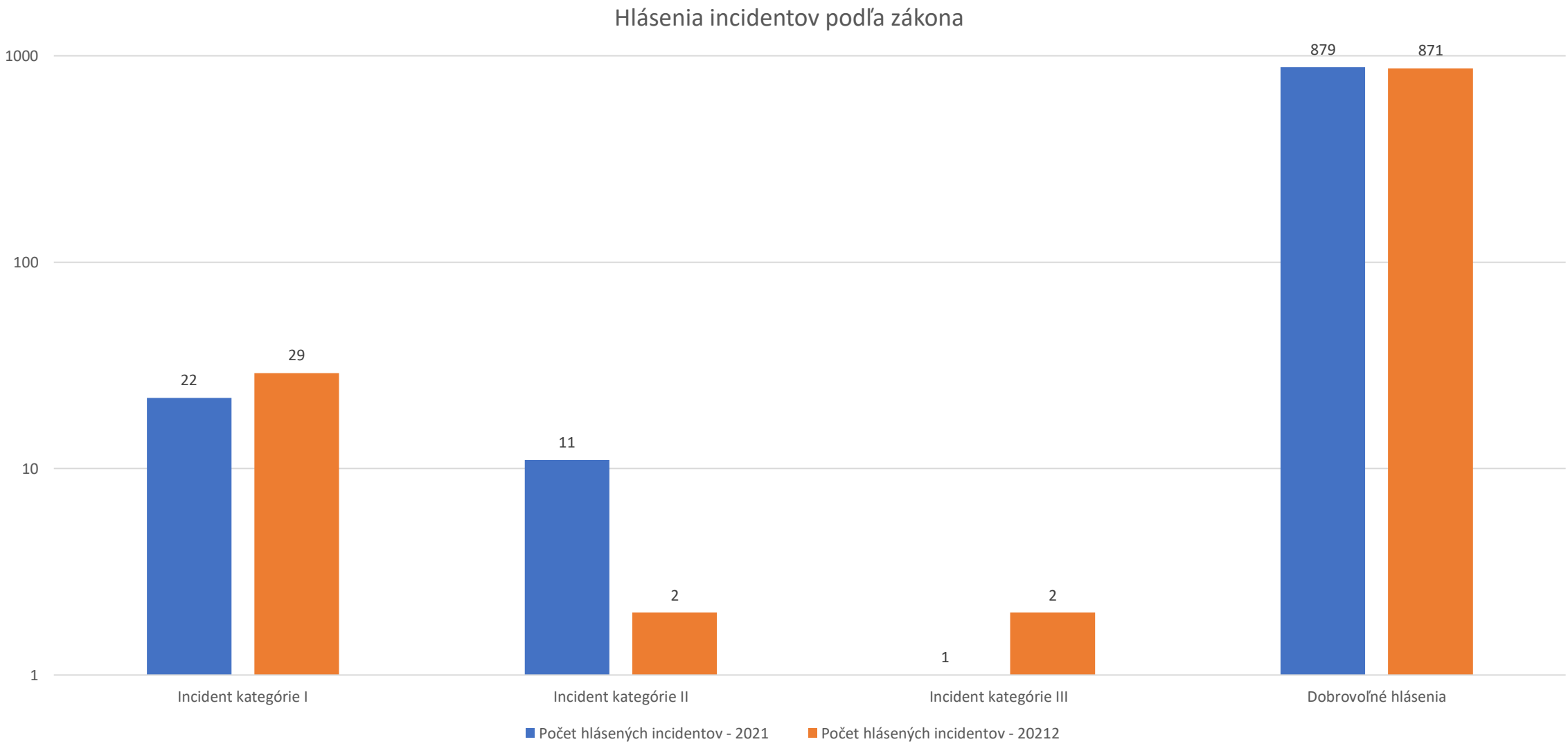
DDoS

- Plánované aj neplánované výpadky
- Veľké výpadky z ne-kyber dôvodov
- Ransom DDoS – nezaplatíš, zaútočíme

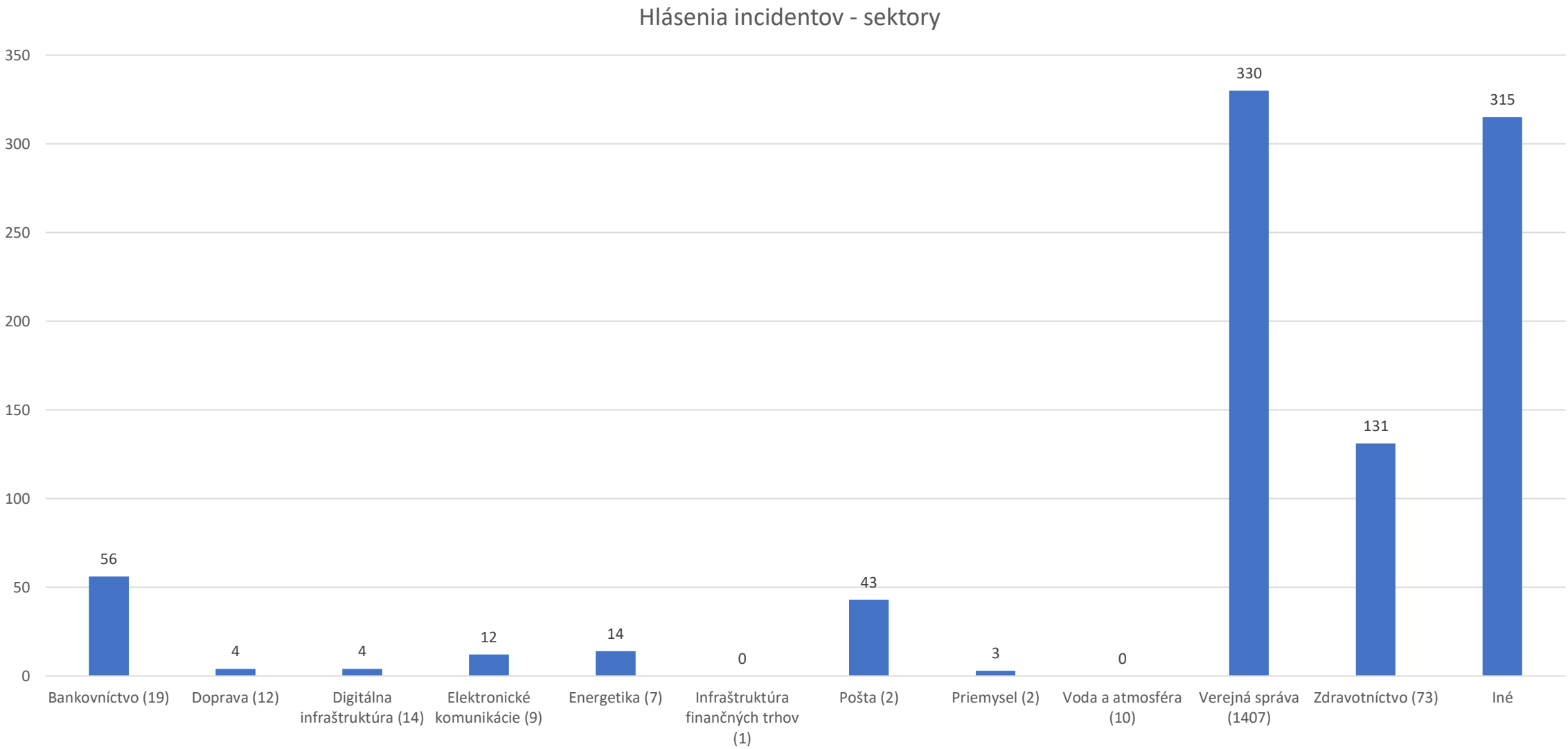
DETEGOVANÉ A RIEŠENÉ INCIDENTY



HLÁSENÉ INCIDENTY PODĽA ZÁKONA



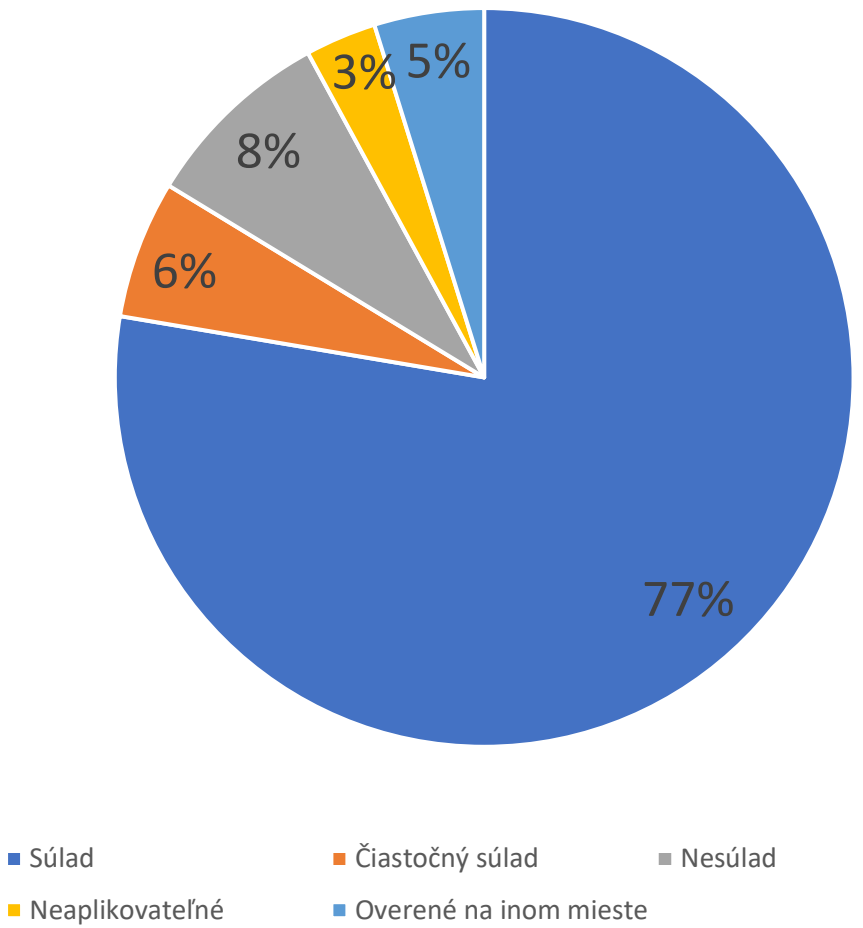
HLÁSENÉ INCIDENTY - SEKTORY



SEKTOROVÝ POHĽAD
(VYBRANÉ SEKTORY)

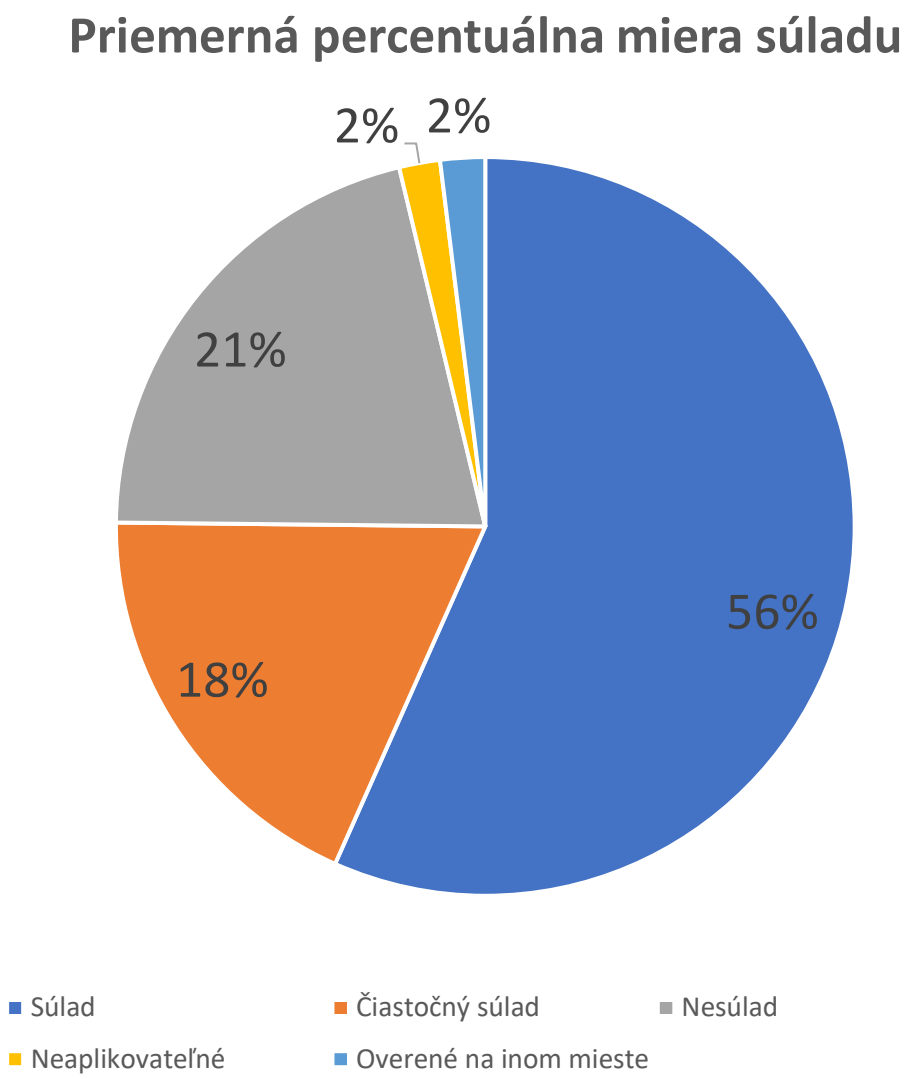
BANKOVNÍCTVO

- Sektor s dlhodobo dobrými výsledkami v oblasti kybernetickej bezpečnosti
- Faktor ovplyvňujúci zvyšovanie kybernetickej bezpečnosti – **legislatívne požiadavky**
- Implementácia bezpečnostných opatrení nad rámec zákona
- BCM prítomné „as normal“
- Vysoká miera súladu s auditnými požiadavkami



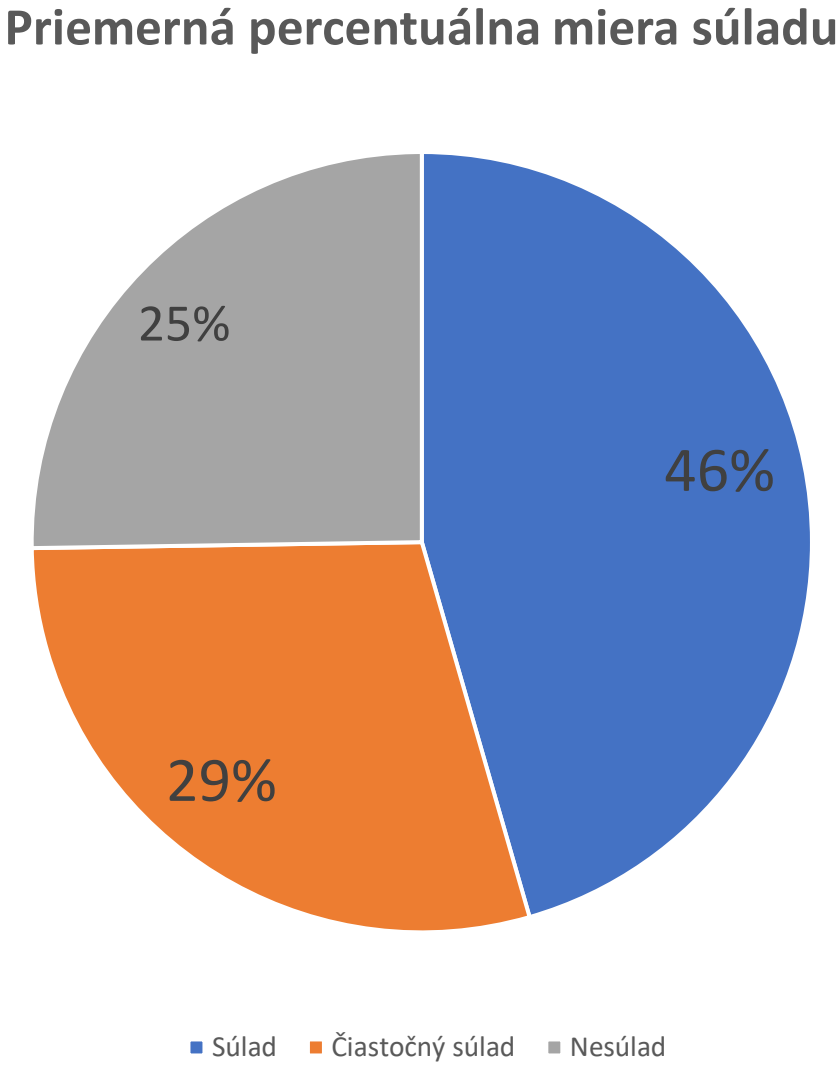
ENERGETIKA

- Veľké rozdiely medzi podsektormi aj v rámci podsektorov
- Elektroenergetika – väčšina prevádzkovateľov vysoký súlad, avšak 35% má veľmi nízku mieru súladu
- Tepelná energetika – najhorší podsektor v miere súladu, priemer 0,82%, dvaja prevádzkovatelia s nulovým súladom



VEREJNÁ SPRÁVA

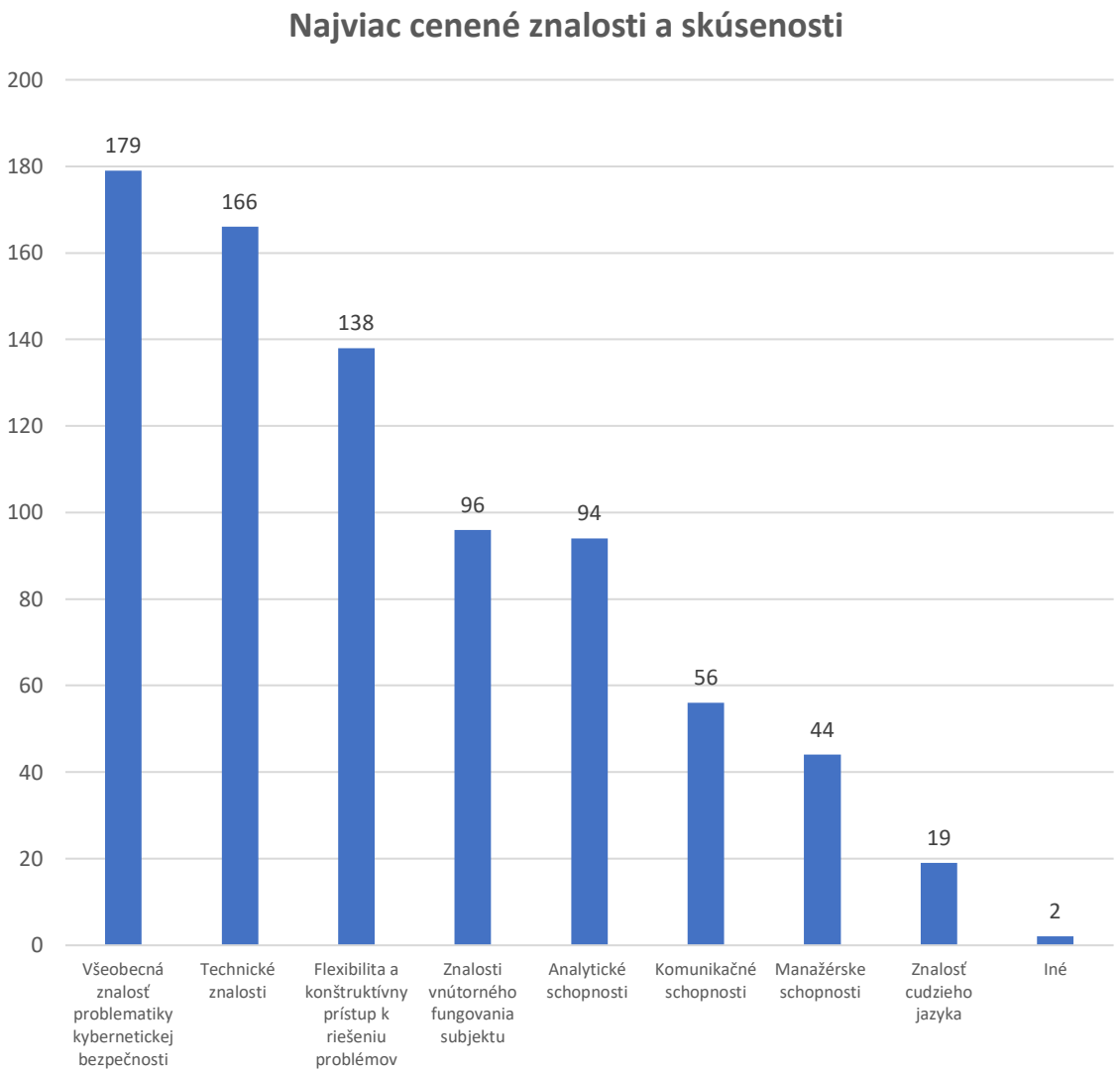
- dlhodobo vykazuje vysokú mieru zanedbávania témy kybernetickej bezpečnosti
- veľmi laxný prístup k tejto problematike, ktorú berú iba ako ďalšiu reguláciu zo strany štátu
- analýza rizík býva často povrchná, vytváraná genericky externou spoločnosťou
- Najčastejšie nálezy z auditov
  - Nebol preukázaný systém riadenia kybernetickej bezpečnosti
  - Bezpečnostná stratégia kybernetickej bezpečnosti ani ďalšia bezpečnostná dokumentácia nebola predložená
  - Analýza rizík nie je zakotvená ako proces v interných predpisoch ani metodicky popísaná, nevykonáva sa

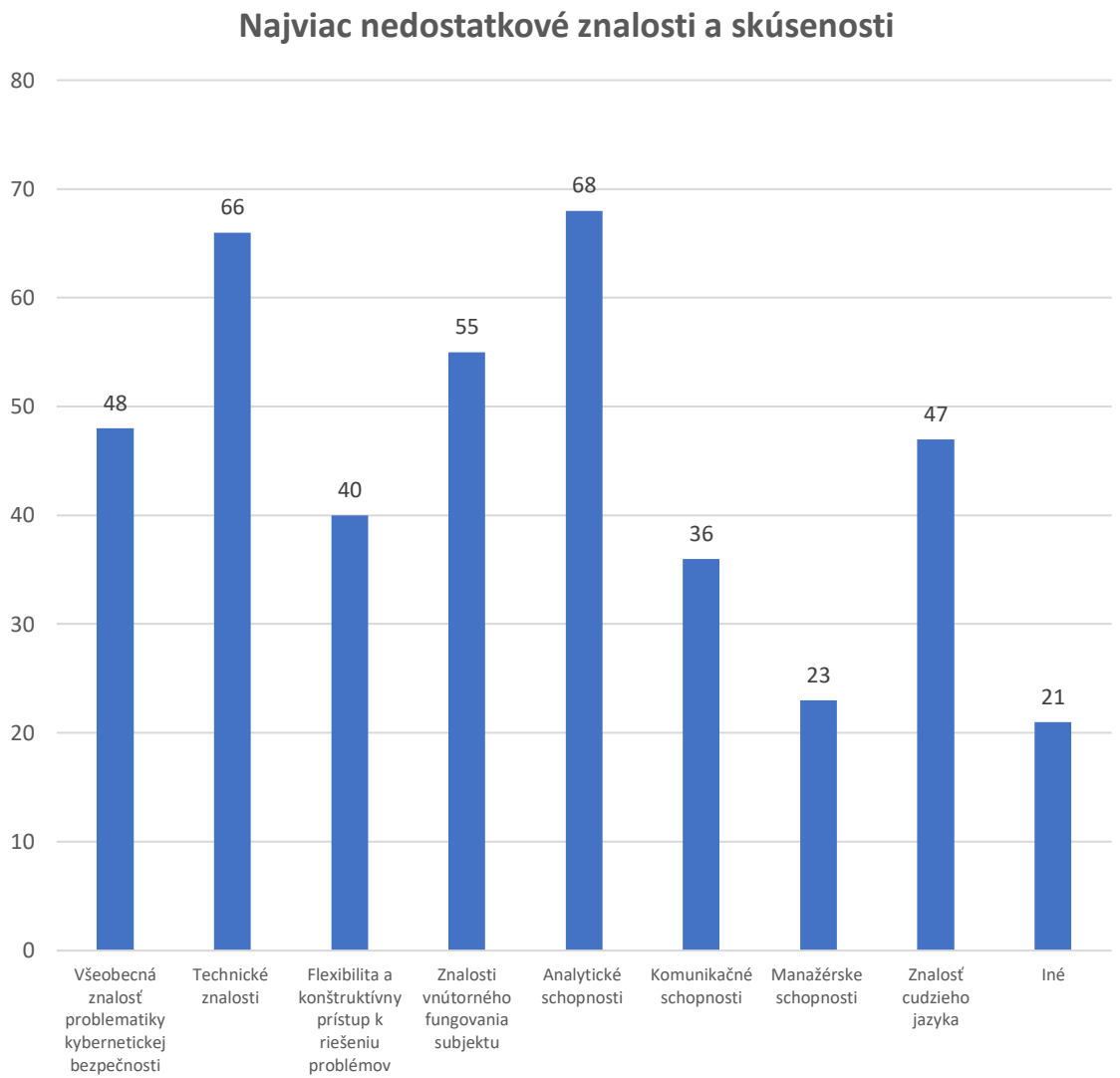


ZAMESTNANOSŤ

- Dáta z profesia.sk
- 40 294 inzerovaných ponúk v oblasti IT
  - 13,8% zo všetkých ponúk na profesia.sk
  - 115 770 reakcií
- špecialista IT bezpečnosti - 1739 ponúk
  - 4,3% zo všetkých ponúk na profesia.sk
  - 3409 reakcií
- Ponuky v kyberbezpečnosti – 372
  - 234 reakcií
- Najčastejšie pozície - Špecialista IT bezpečnosti, Senior Analytik pre Kybernetickú bezpečnosť, Cybersecurity Operations - Incident Response Specialist, Cyber Security Consultant, Cybersecurity Architect - Cybersecurity Operations

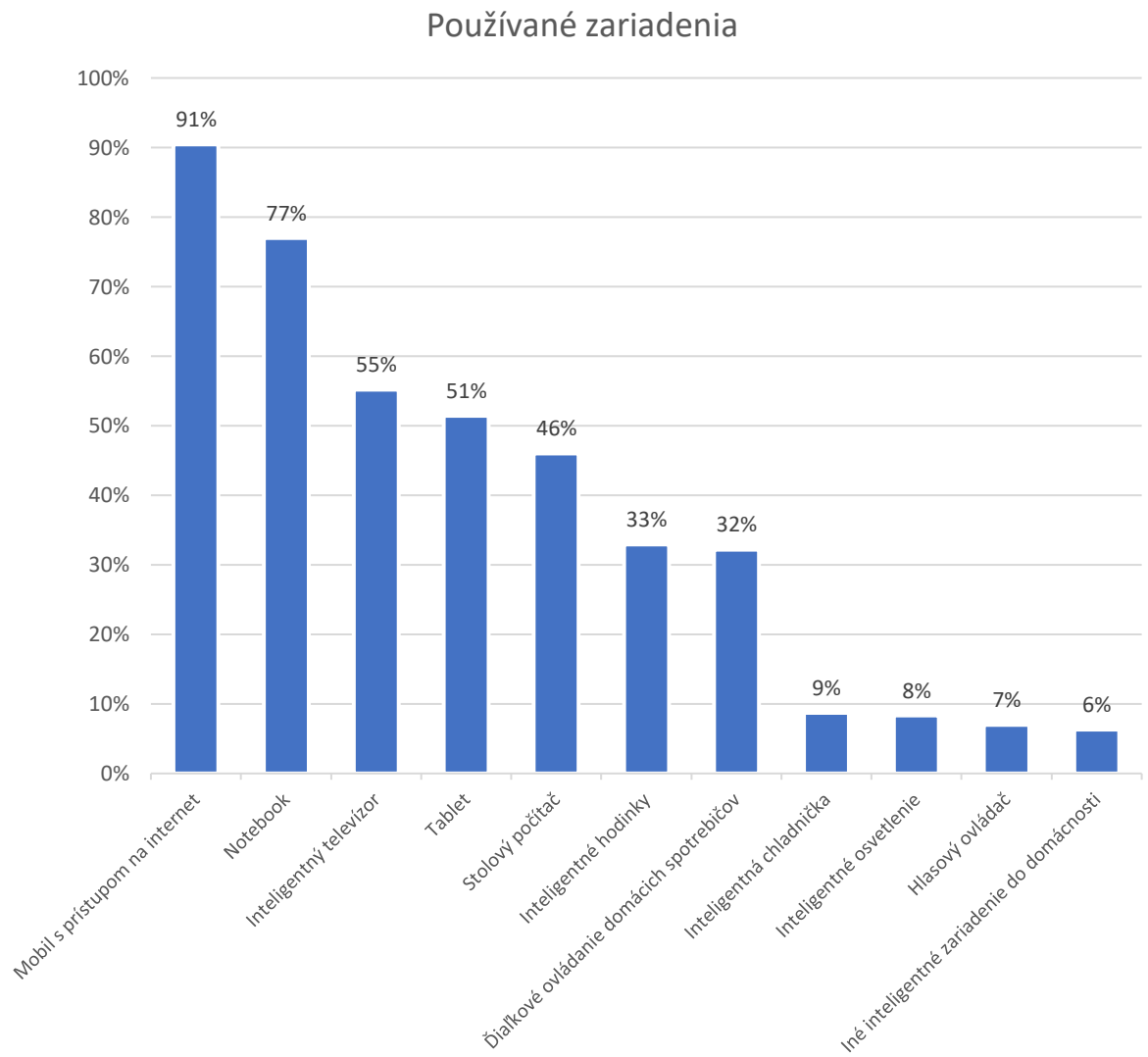
POTREBY PZS


Najviac cenené znalosti a skúsenosti
200
180
160
140
120
100
80
60
40
20
0
179
166
138
96
94
56
44
19
2
Všeobecná znalosť problematiky kybernetickej bezpečnosti
Technické znalosti
Flexibilita a konštruktívny prístup k riešeniu problémov
Znalosti vnútorného fungovania subjektu
Analytické schopnosti
Komunikačné schopnosti
Manažérske schopnosti
Znalosť cudzieho jazyka
Iné


Najviac nedostatkové znalosti a skúsenosti
80
70
60
50
40
30
20
10
0
48
66
40
55
68
36
23
47
21
Všeobecná znalosť problematiky kybernetickej bezpečnosti
Technické znalosti
Flexibilita a konštruktívny prístup k riešeniu problémov
Znalosti vnútorného fungovania subjektu
Analytické schopnosti
Komunikačné schopnosti
Manažérske schopnosti
Znalosť cudzieho jazyka
Iné

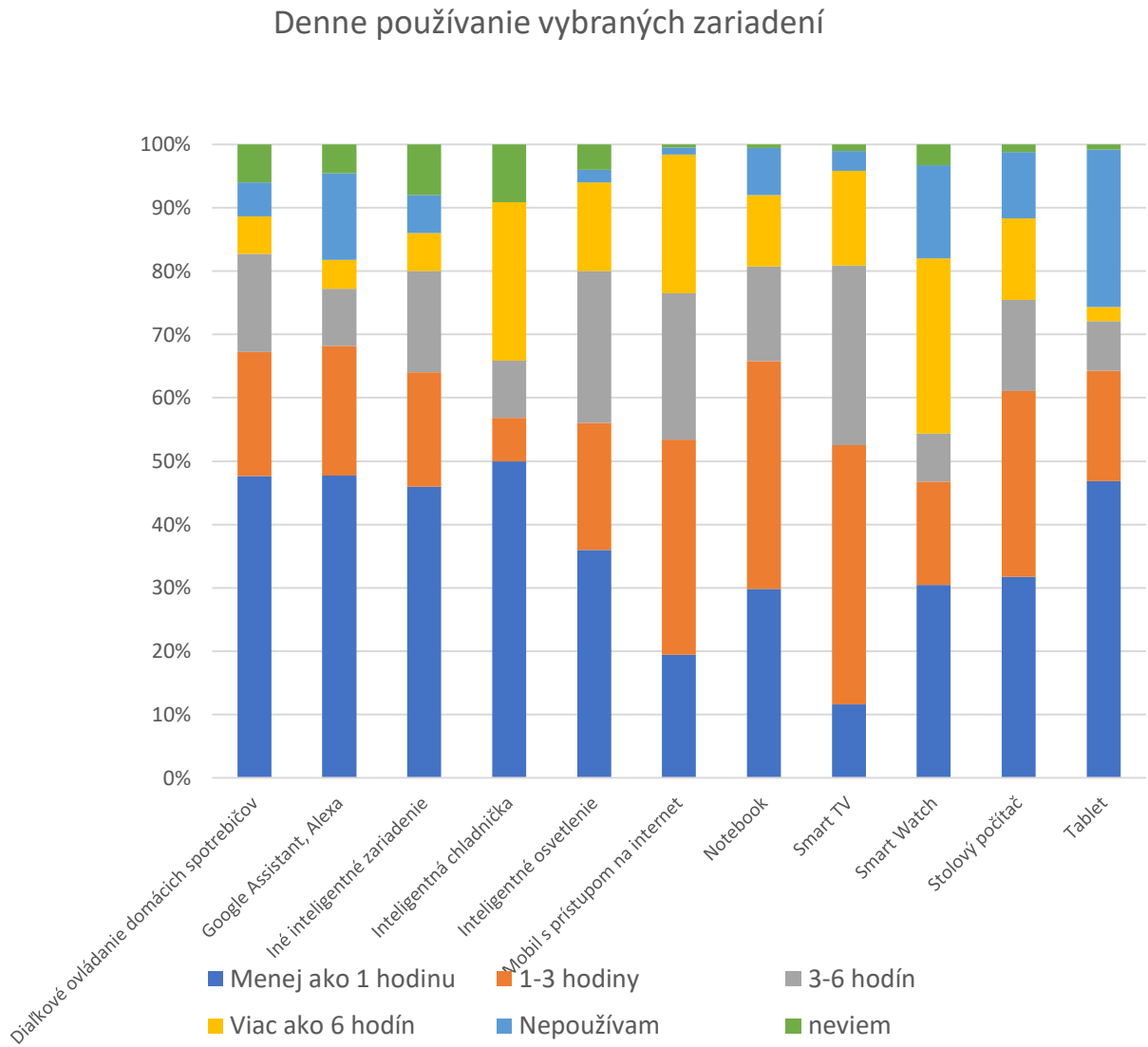
VEREJNOSŤ – POUŽÍVANÉ ZARIADENIA

- Ústup stolných počítačov
- Nástup „smart“ zariadení a IoT
- Nárast mobilných zariadení (mobily, tablety, notebooky)
- Zvyšujúca sa digitalizácia domácností

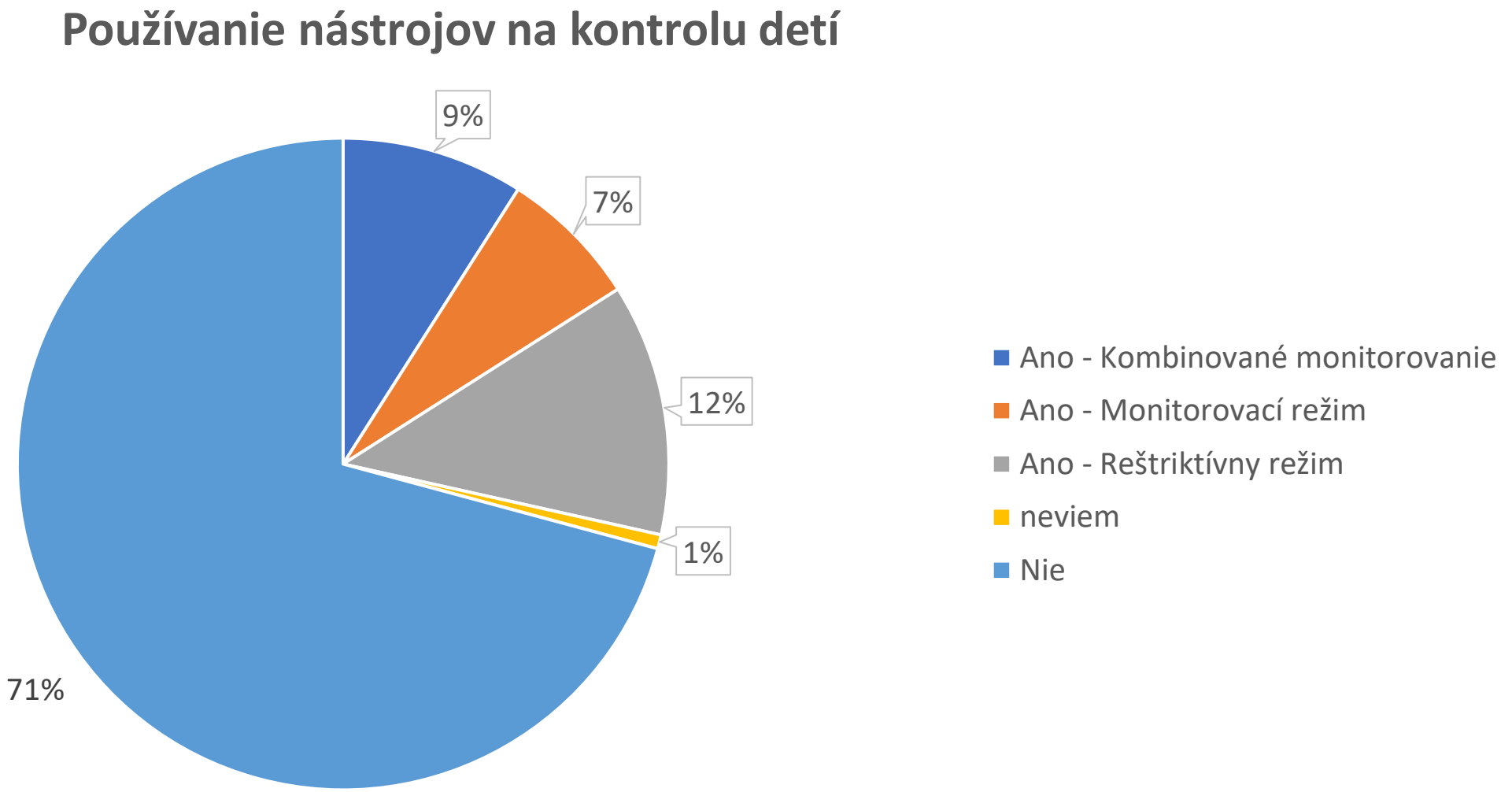


VEREJNOSŤ – POUŽÍVANÉ ZARIADENIA

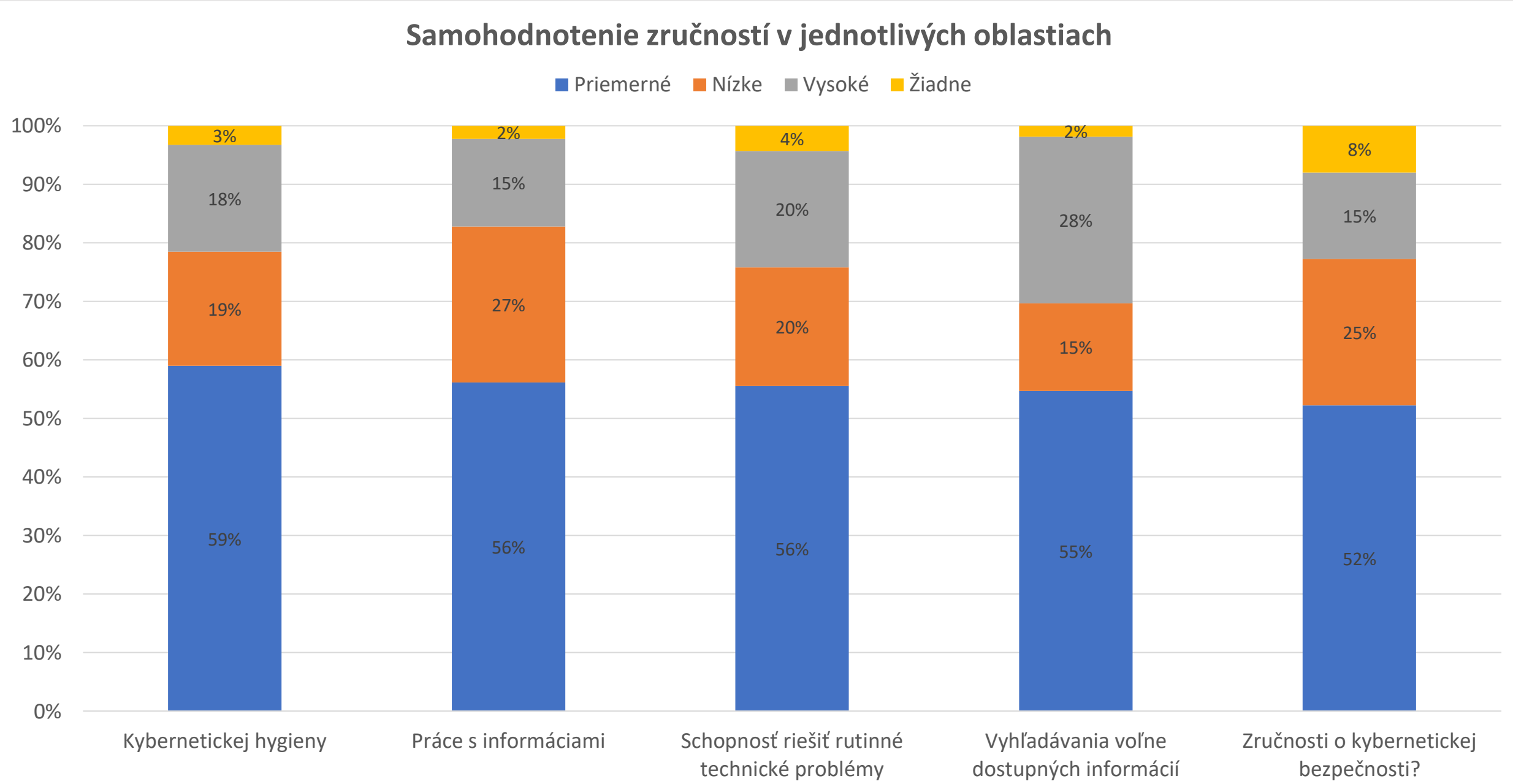
- Väčšina zariadení používaná od 1 do 3 hodín
- Mobilný telefón ako najpoužívanejšie zariadenie
- Nezapočítané niektoré aspekty (práca, „používanie“ chladničky)



VEREJNOSŤ – RODIČOVSKÁ KONTROLA



VEREJNOSŤ – SAMOHODNOTENIE ZRUČNOSTÍ



AKTIVITY – BULLETINY A VAROVANIA

	TÝŽDENNÉ BEZPEČNOSTNÉ BULLETINY				BEZPEČNOSTNÉ VAROVANIA			
	Celkový počet bulletinov	Stredná	Vysoká	Spolu zraniteľností		Vysoká	Kritická	Spolu varovaní
Január	4	4	30	34	**Január**	0	19	19
Február	4	1	36	37	**Február**	0	29	29
Marec	5	3	60	63	**Marec**	2	21	23
Apríl	5	2	48	50	**Apríl**	3	18	21
Máj	4	1	31	32	**Máj**	7	18	25
Jún	5	0	33	33	**Jún**	4	18	22
Júl	4	0	25	25	**Júl**	9	25	34
August	5	0	38	38	**August**	7	25	32
September	4	0	26	26	**September**	14	17	31
Október	4	0	22	22	**Október**	8	17	25
November	5	0	32	32	**November**	5	19	24
December	4	0	24	24	**December**	2	17	19
SPOLU	**53**	**11**	**405**	**416**	**SPOLU**	**61**	**243**	**304**

AKTIVITY – NÁRODNÁ SPOLUPRÁCA

- Spolupráca s relevantnými subjektami (SIS, VS, NASES, PZ, MIRRI)
- Riešenie a koordinácia riešenia kybernetických bezpečnostných incidentov
- Komunikačná platforma pre PZS – zdieľanie skúseností, výmena odporúčaní, pripomienkovanie zásadných dokumentov
- Sprístupnenie TaranisNG (www.taranis.ng)
  - Agregácia a analýza informácií z otvorených zdrojov
  - Open Source softvér
- Aktívna účasť na konferenciách, workshopoch, prednáškach, ich organizovanie
- Aktívna účasť na medzinárodných cvičeniach

AKTIVITY – MEDZINÁRODNÁ SPOLUPRÁCA

- NBÚ – hlavný kontaktný bod pre zahraničných partnerov
  - Rada EÚ HWPCI, NIS Cooperation Group, CSIRT Network, CyCLONe, ENISA
  - NATO, OBSE, ESCO, CECSP
- NCKB SK-CERT – člen Trusted Introducer (Certified) a FIRST
- Podieľanie sa na medzinárodných aktivitách
  - Operatívna výmena informácií
  - Účasť na medzinárodných konferenciách, pracovných skupinách a iných formátoch
  - Spolupráca pri riešení incidentov s cezhraničným presahom

AKTIVITY – NÁRODNÁ STRATÉGIA KYBERNETICKEJ BEZPEČNOSTI NA ROKY 2021 AŽ 2025

- 7. januára 2021 schválená vládou
- 7 strategických cieľov (prioritných oblastí):
  - Dôveryhodný štát pripravený na hrozby
  - Efektívne odhaľovanie a objasňovanie počítačovej kriminality
  - Odolný súkromný sektor
  - Kybernetická bezpečnosť ako základná súčasť verejnej správy
  - Silné partnerstvá
  - Vzdelaní odborníci a verejnosť
  - Výskum a vývoj v oblasti kybernetickej bezpečnosti
- Definovanie zahranično-politických partnerov, spôsob implementácie, financovanie
- Akčný plán implementácie – schválený 14. júla 2021, tvorený komunitou
- Monitorovací výbor – monitoruje napĺňanie Akčného plánu

THANKS!

Matej Šalmík

matej.salmik@nbu.gov.sk

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

SK CERT