

ZVÝŠENIE ODOLNOSTI SLOVENSKA VOČI HYBRIDNÝM HROZBÁM POMOCOU POSILNENIA KAPACÍT VEREJNEJ SPRÁVY



Operačný program
**Efektívna
verejná správa**



Európska únia
Európsky sociálny fond



**AKADÉMIA
POLICAJNÉHO ZBORU
V BRATISLAVE**

ZVÝŠENIE ODOLNOSTI SLOVENSKA VOČI HYBRIDNÝM HROZBÁM POMOCOU POSILNENIA KAPACÍT VEREJNEJ SPRÁVY

Kód projektu : 314011CDW7

Realizácia projektu v rámci operačného programu „Efektívna verejná správa“
financovaného z Európskeho sociálneho fondu



**AKADÉMIA
POLICAJNÉHO ZBORU
V BRATISLAVE**



Operačný program
**Efektívna
verejná správa**



Európska únia
Európsky sociálny fond

KYBERNETICKÝ ROZMER HYBRIDNÝCH HROZIEB VO VZŤAHU K VEREJNEJ SPRÁVE

MODUL - 3

HYBRIDNÉ HROZBY – ŠPECIALIZÁCIA PRE ZAMESTNANCOV VEREJNEJ SPRÁVY

doc. Ing. Stanislav Šišulák, PhD., MBA

Bratislava 2023

Cieľ prednášky

Verejná správa je oblasť zodpovedná za riadenie verejných záležitostí, správu štátu a verejných služieb pre občanov. V rámci tohto kontextu sa verejná správa stretáva s výzvami, ktoré prichádzajú s hybridnými hrozbami. Tieto hrozby môžu zasiahnuť rôzne oblasti verejnej správy a spoločnosti ako celku. Hybridné hrozby sú zvlášť nebezpečné pre verejnú správu, pretože môžu oslabiť spoločnosť a jej inštitúcie, destabilizovať politický systém a spôsobiť nedôveru občanov voči vláde.

Kybernetický rozmer hybridných hrozieb vo verejnej správe je významný a predstavuje jednu z najväčších výziev. Kybernetické útoky sa stávajú čoraz sofistikovanejšími a šíria sa rýchlejšie ako kedykoľvek predtým. Ich cieľom je narušiť, poškodiť alebo získavať neoprávnený prístup k dátam a informačným systémom verejnej správy. Pre verejnú správu je dôležité venovať pozornosť hybridným hrozbám a vyvíjať opatrenia na ich predchádzanie a zvládanie. To zahŕňa posilnenie kybernetickej bezpečnosti, zlepšenie informačnej gramotnosti a kritického myslenia občanov, budovanie odolnosti voči dezinformáciám a manipulácii s verejnou mienkou, a zlepšenie spolupráce medzi rôznymi inštitúciami na boj proti hybridným hrozbám. Verejná správa využíva informačné technológie na spracovanie a uchovávanie citlivých údajov, ako sú osobné údaje občanov, dôverné informácie a utajované skutočnosti. Kybernetické útoky na tieto systémy môžu spôsobiť značné škody a ohroziť dôveru verejnosti v inštitúcie verejnej správy.

Pre boj proti kybernetickým hrozbám vo verejnej správe je dôležité implementovať silné bezpečnostné opatrenia, vrátane viacúrovňovej autentifikácie, šifrovania, monitorovania sietí a systémov, aktualizácie softvéru a vytvorenie kultúry kybernetickej bezpečnosti medzi zamestnancami. Spolupráca s odborníkmi na kybernetickú bezpečnosť a kontinuálne zlepšovanie bezpečnostných opatrení je nevyhnutná pre ochranu informačných systémov verejnej správy pred kybernetickými hrozbami.

Obsah

1. Informačná a kybernetická bezpečnosť, ciele, model a strategické aktíva organizácie
2. Útoky na kritickú infraštruktúru verejnej správy ako jeden z nástrojov hybridných hrozieb
3. Bezpečnosť informačných technológií vo verejnej správe
4. Informačný systém krízového manažmentu verejnej správy a nástroje na znižovanie rizika pred HH
5. Príklady najčastejších útokov vo verejnej správe
6. Platforma „Tik – Tok“ zábava alebo hybridná hrozba
7. Príklad hybridnej hrozby použitím špionážneho softvéru „Pegasus“ a reakcia Európskej únie
8. Blíži sa ďalšia úroveň umelej inteligencie „AI“ a naša demokracia nie je pripravená
9. Reakcia NATO a ochrana kybernetických sietí proti hybridným hrozbám
10. Bezpečnostné incidenty NBÚ, CSIRT, SK-CERT, vzdelávanie

1. Informačná a kybernetická bezpečnosť, ciele, model a strategické aktíva organizácie

Informačnú bezpečnosť - je možné definovať ako „zachovanie dôvernosti, integrity a dostupnosti informácií“.

Kybernetická bezpečnosť ako „zachovanie dôvernosti, integrity a dostupnosti informácií v kybernetickom priestore“.

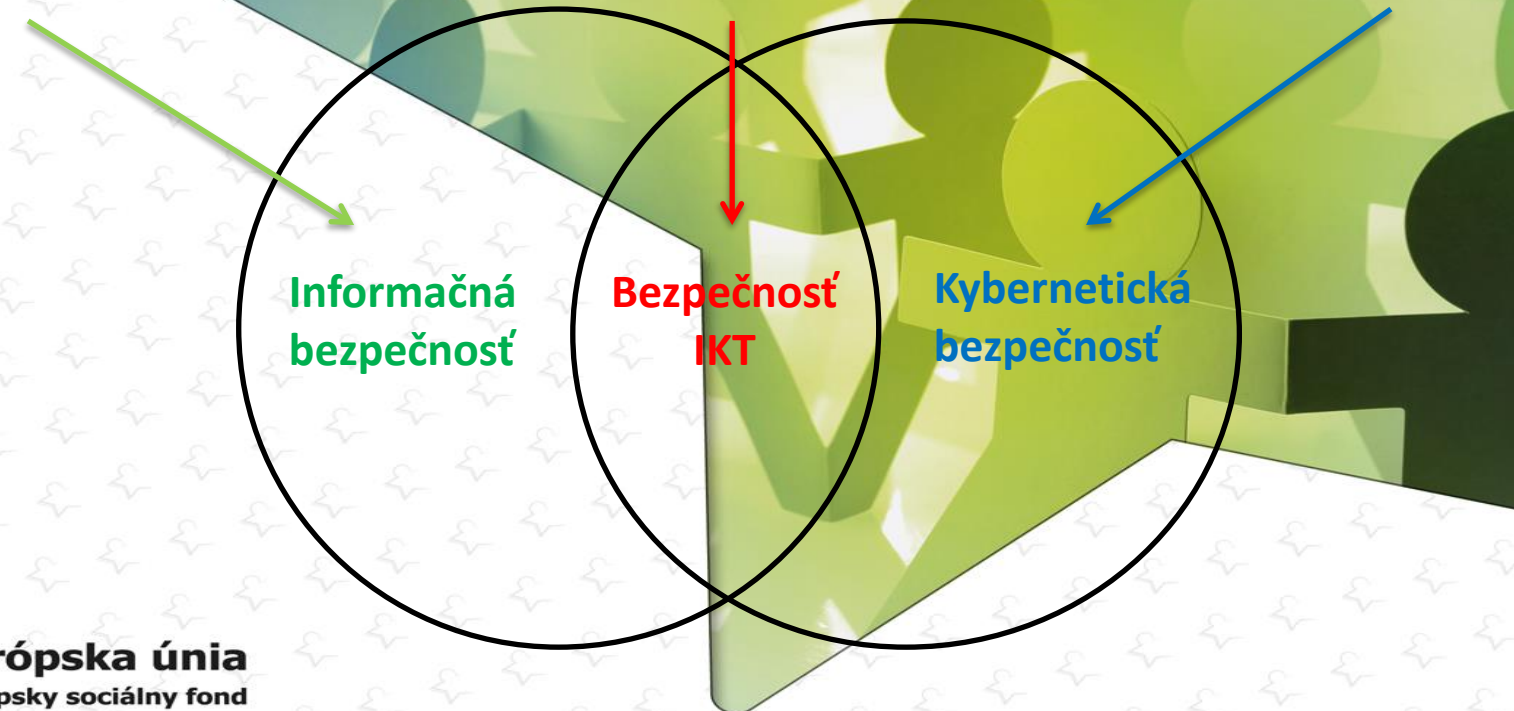
Kybernetický priestor - je „komplexné prostredie, ktoré je výsledkom interakcie ľudí, softvéru a služieb na internete prostredníctvom technologických zariadení a sietí, ktoré sú k nemu pripojené, a ktoré neexistujú v žiadnej fyzickej podobe“.

Rozdiel medzi informačnou a kybernetickou bezpečnosťou

Aktíva v podobe informácií ukladané alebo prenášané bez použitia IKT

Aktíva v podobe informácií ukladané alebo prenášané s použitím IKT

Neinformačné aktíva zraniteľné voči hrozbám prostredníctvom IKT



Ciele informačnej a kybernetickej bezpečnosti

Dôvernosť (confidentiality) - zabezpečenie dôvernosti znamená, že dôverné informácie nie sú prístupné alebo zverejnené neoprávneným osobám, subjektom alebo procesom.

Celistvosť (integrity) - tento cieľ sa dosiahne v tom prípade, keď sa zabezpečia kompletne, konzistentné a nemodifikované informácie.

Dostupnosť (availability) podstatou tohto cieľa je, aby informácie boli prístupné a použiteľné v správny čas, na správnom mieste, oprávnenej osobe, subjektu alebo procesu, a existujú prekážky

Držba alebo kontrola (possession or control) - týkajúca sa fyzického nakladania s médiom, na ktorom sú informácie uložené

Autenticita (authenticity) - tento princíp nám umožňuje povedať, či sú príslušné informácie pripísané správnejmu vlastníkovi alebo

Užitočnosť (utility) - odkazuje na to, ako užitočné sú informácie.

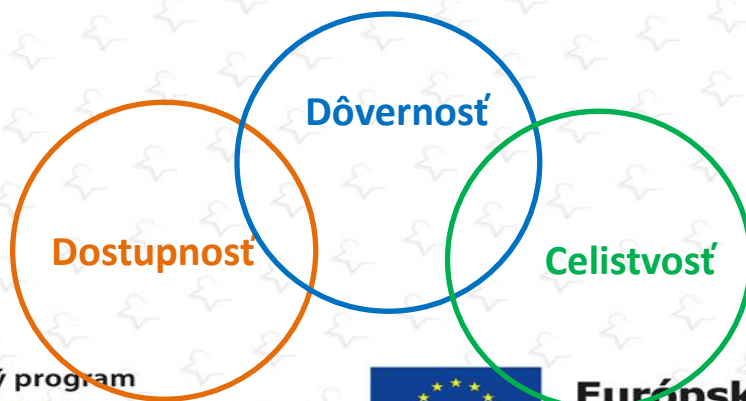
TRIÁDA - CIA



Operačný program
**Efektívna
verejná správa**



Európska únia
Európsky sociálny fond

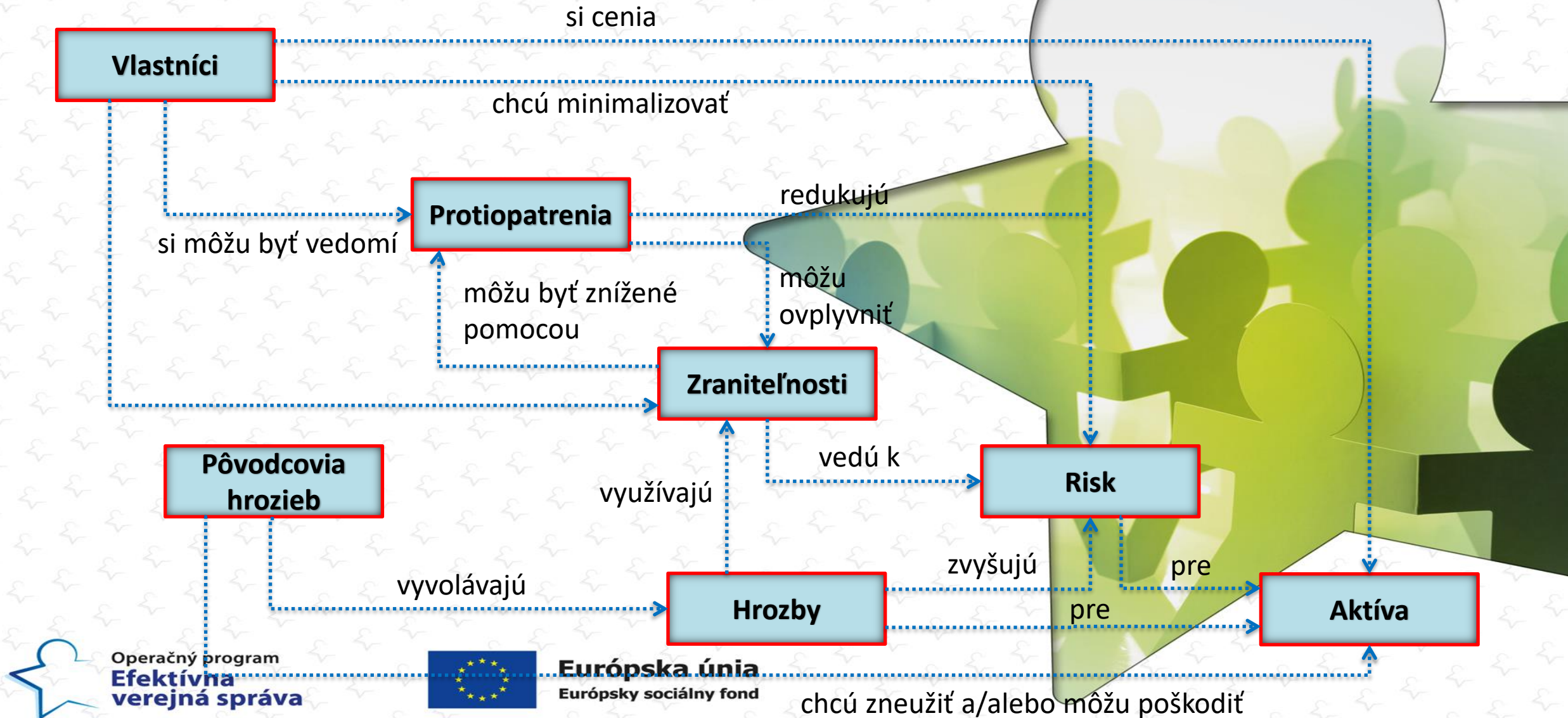


PARKERIANOVA
ŠESTICA



Model informačnej a kybernetickej bezpečnosti

International Organization for Standardization, International Electrotechnical Commission. ISO/IEC 15408-1:2005 Information technology — Security techniques — Evaluation criteria for IT security



Strategické aktíva organizácie

- **informácie** - osobné údaje, strategické informácie alebo veľmi nákladné informácie,
- **procesy a činnosti** - procesy, ktoré obsahujú obchodné tajomstvá alebo zahŕňajú duševné vlastníctvo,
- **hardvér** - zariadenia na spracovanie dát, prenosné zariadenia, pevné zariadenia.....,
- **softvérové vybavenie** - operačný systém, aplikácie (napr. SAP) Systém na správu webového obsahu alebo samotný kód webovej stránky organizácie (napr. ústredný portál verejnej správy),
- **komunikačné siete** - prenosové médium a jeho podpora (napr. optický kábel), pasívne alebo aktívne prenosové zariadenia (napr. WiFi smerovač - router),
- **pracovníci a ich know-how** - osoby, ktoré rozhodujú o činnosti organizácie, osoby v pozícii používateľov IS, osoby v rámci prevádzky alebo údržby a vývojárov IS.

2. Útoky na kritickú infraštruktúru verejnej správy ako jeden z nástrojov hybridných hrozieb

- externý alebo interný politický nátlak na najvyšších štátnych predstaviteľov a štátne inštitúcie,
- ekonomický alebo energetický nátlak ako rozšírenie politického nátlaku,
- rozsiahle sabotáže proti kľúčovej infraštruktúre,
- kybernetické útoky s potenciálom spôsobiť škody veľkého rozsahu,
- informačné a propagandistické operácie s cieľom podkopať dôveru v štátne inštitúcie, vyvolať spoločenské nepokoje a vážne destabilizovať politickú a bezpečnostnú stabilitu,
- ovplyvňovanie etnických, náboženských a kultúrnych menšín a ich manipulácia na politické účely,
- hrozba použitia vojenskej sily,
- aktivity nepravidelných/polovojenských ozbrojených skupín nelojálnych k štátu,
- výzvedné a podvratné aktivity tajných služieb,
- strategická korupcia využívaná s politickými cieľmi a motívmi,
- ovplyvňovanie volebných procesov cudzou mocou.



Operačný program

Efektívna

správa



Európska únia

Európsky sociálny fond

3. Bezpečnosť informačných technológií vo verejnej správe

- zákon č. **95/2019** Z.z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov,
- centrálnym metainformačným systémom VS je IS VS, ktorého obsahom sú najmä technologické, administratívne a organizačné údaje o prevádzkovaných informačných technológiách VS,
- správcom vládneho elektronického komunikačného systému Govnet je Ministerstvo investícií regionálneho rozvoja a informatizácie SR,
- cieľom je dbať na vytvorenie integrovaného prostredia informačných technológií VS,
- správca, ktorý je prevádzkovateľom základnej služby, prijíma a realizuje bezpečnostné opatrenia vo vzťahu k IS VS v jeho správe podľa tohto zákona,
- plánovanie, obstarávanie, implementácia, prevádzka, servis, podpora, monitoring, hodnotenie, štandardy, výklad, vládny cloud, Govnet, číselníky, elektronický odpis a výstup.

4. Informačný systém krízového manažmentu VS a nástroje na znižovanie rizika zraniteľnosti pred hybridnými hrozbami

Vytváranie informácií:

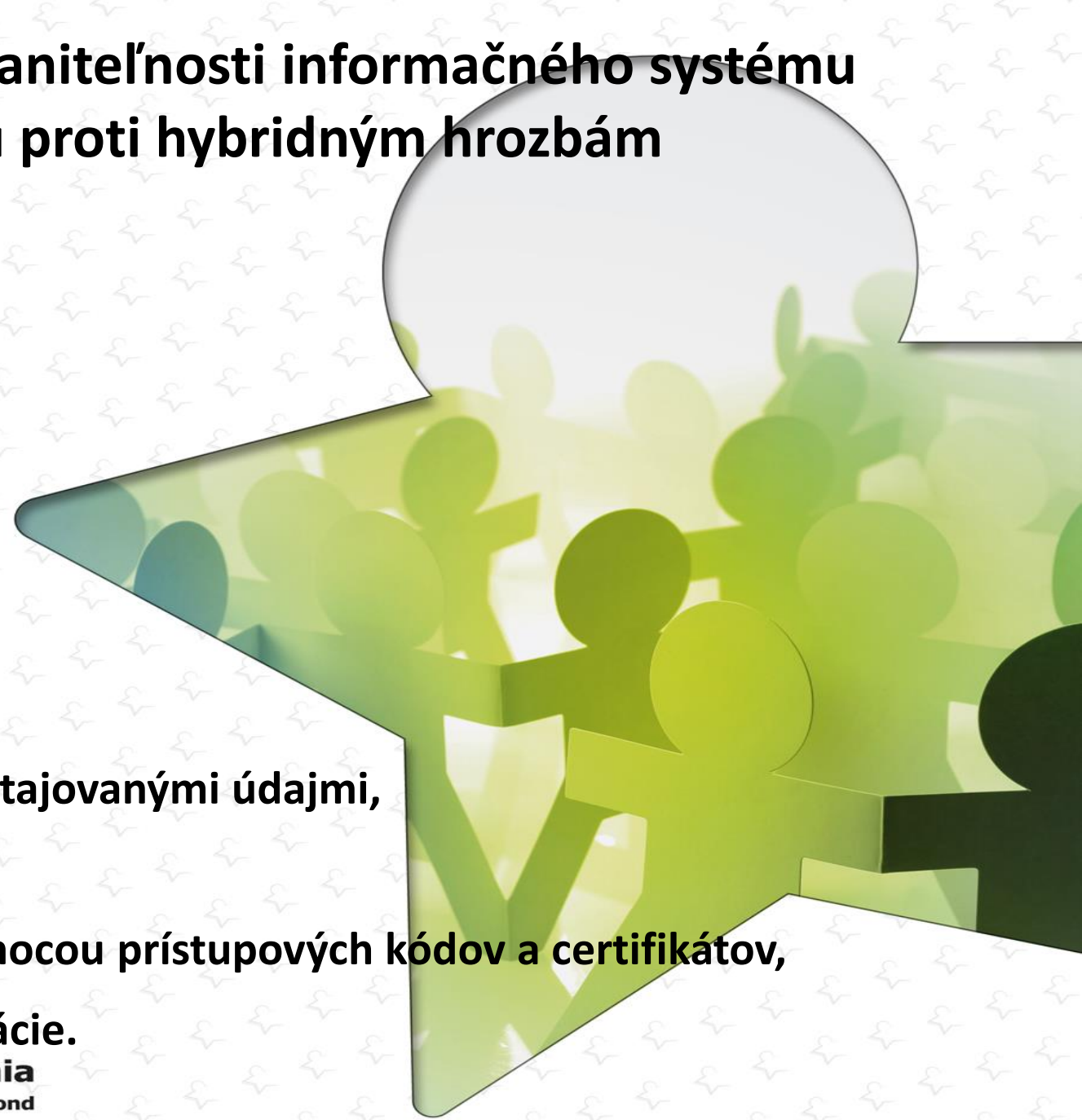
- vytváranie a naplňovanie databáz informáciami potrebnými na riešenie krízových javov ,
- prevádzkovanie systému trvalého monitorovania krízových činiteľov,
- sprostredkovanie informácií ,
- odovzdávanie informácií prostredníctvom počítačových sietí (program hospodárskej mobilizácie),
- vytvorenie systému pravidelných hlásení (písomne, telefonicky, osobne),
- prevádzkovanie varovacej a vyznamievacej siete CO,
- odovzdanie oficiálnych informácií pre hromadné oznamovacie prostriedky,
- spracovanie informácií od fyzických alebo právnických osôb, ktoré sa stali účastníkmi krízových javov.

Riziká zraniteľnosti:

- podceňovanie bezpečnostných rizík zo strany zodpovedných funkcionárov,
- absencia analýz ohrození, prevencie, krízových plánov, ich materiálo technického zabezpečenia,
- neznalosť systému KM s následnými problémami pri organizovaní a riadení záchranných prác,
- problémy so zapojením občanov do riešenia krízy a s prijímaním účinných opatrení na ich záchranu,
- prípravenosť občanov reagovať na jednotlivé stupne výstrah (varovné signály a činnosti na ne).

Nástroje na znižovanie rizika zraniteľnosti informačného systému krízového manažmentu proti hybridným hrozbám

- univerzálnosť,
- odolnosť,
- bezpečnosť,
- modifikovateľnosť,
- jednoznačnosť v správe dát,
- hierarchia zdrojov dát,
- dodávateľ informačného systému,
- podmienky na prácu s neutajovanými aj utajovanými údajmi,
- zálohovanie údajov,
- zabezpečenie autentizácie užívateľov pomocou prístupových kódov a certifikátov,
- technické podmienky šifrovanej komunikácie.



5. Príklady najčastejších útokov vo verejnej správe

Typ útoku : **SOCIÁLNE INŽINIERSTVO**

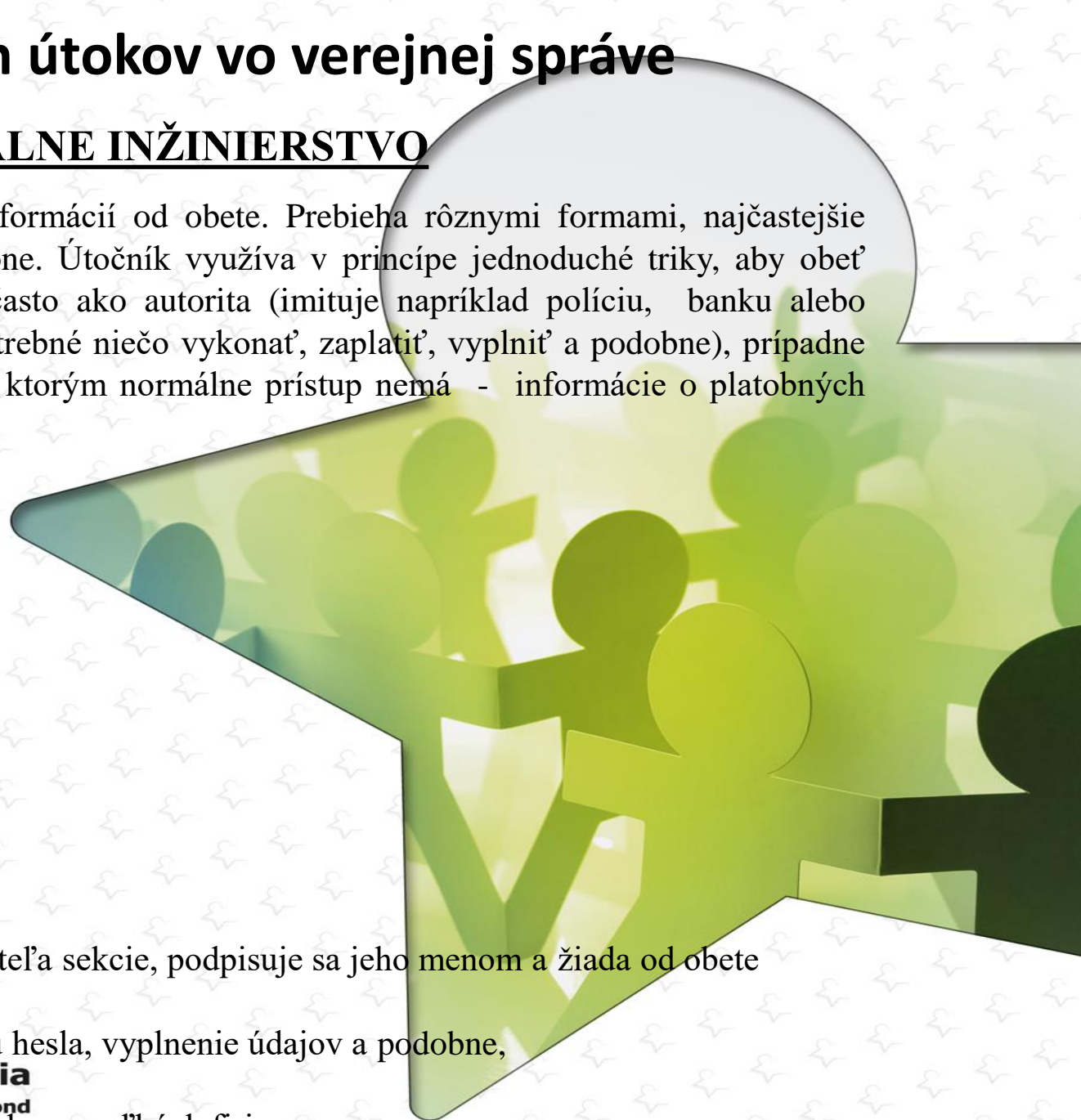
Popis: Sociálne inžinierstvo je úspešný spôsob získania informácií od obete. Prebieha rôznymi formami, najčastejšie phishingovými e-mailami, vishingovými telefonátmi a podobne. Útočník využíva v princípe jednoduché triky, aby obeť presvedčil na konanie, ktoré útočník potrebuje. Vystupuje často ako autorita (imituje napríklad políciu, banku alebo zamestnávateľa), dáva urgentné požiadavky (teraz hneď je potrebné niečo vykonať, zaplatiť, vyplniť a podobne), prípadne sľubuje odmenu. Cieľom útočníka je dostať sa k údajom, ku ktorým normálne prístup nemá - informácie o platobných kartách, prihlasovacie údaje do systémov a služieb a podobne.

Riešenia/Opatrenia:

- pravidelné školenia zamestnancov, vrátane manažmentu,
- dobré bezpečnostné politiky,
 - o oddeľovanie rolí a zodpovedností,
 - o manažment prístupov,
 - o dobrá politika hesiel a dvojfaktorová autentifikácia,
- technické opatrenia,
 - o antispamové filtre,
 - o ochrana na koncových zariadeniach.

Príklady

- útočník imituje zamestnávateľa/generálneho riaditeľa/riaditeľa sekcie, podpisuje sa jeho menom a žiada od obete (zamestnanca) platbu, vyplnenie formulára a podobne,
- útočník imituje IT administrátora organizácie, žiada zmenu hesla, vyplnenie údajov a podobne,
- útočník imituje partnerskú organizáciu, žiada citlivé údaje,
- útočník imituje banku/políciu/poštové služby/technickú podporu veľkých firiem.



Typ útoku : INFEKCIA ŠKODLIVÝM KÓDOM

Popis: Škodlivý kód je typicky program alebo jeho časť, ktorý vykonáva malígne činnosti v zariadení, ktoré mu nakonfiguroval útočník. Škodlivý kód môže mať rôzny účel, existuje hneď niekoľko typov škodlivého kódu, každý má iný účel, resp. spôsob vykonávania svojich funkcií. Dnes je najrozšírenejším škodlivým kódom ransomvér, ktorého účelom je zašifrovanie údajov na zariadení obete a následné pýtanie výkupného. Ransomvér je často spojený aj s exfiltráciou dát obete a možnosťou tzv. dvojitého vydierania – zaplať, lebo tvoje údaje zverejním. Existuje však mnoho ďalších typov škodlivého kódu – trojan (legitímne tváriaci sa škodlivý kód), advér, spyware, červy, rootkity, RATy a podobne. Infekcia škodlivým kódom môže nastať rôznymi spôsobmi – v rámci phishingových kampaní, zneužitím zraniteľnosti, zneužitím uniknutých prihlasovacích údajov, priamou inštaláciou na zariadeniach ktoré sú bez autentifikácie voľne dostupné z internetu a podobne.

Riešenia/Opatrenia:

- pravidelná aktualizácia operačného systému a aplikácií,
- nasadenie bezpečnostných technických nástrojov na všetkých úrovniach (sieťová, serverová, koncové zariadenia),
- nepretržitý monitoring siete a vyhodnocovanie udalostí,
- zber a vyhodnocovanie indikátorov kompromitácie (indikátorov, ktoré dokazujú infekciu škodlivým kódom),
- iné technické opatrenia.

Príklady:

- ransomvérové útoky na dôležité subjekty (kritická infraštruktúra),
- inštalácia rootkitov vo významných organizáciách a zber údajov,
- infekcia zariadení a ich zaradenie do siete botnet, kde sú využívané na ďalšie útoky,
- infekcia škodlivým kódom a následné odpočúvanie komunikácie.

Typ útoku : **ZNEUŽITIE ZRANITEĽNOSTI**

Popis: Systémy, softvér a služby sa neustále vyvíjajú, sú pridávané nové funkcie a na výrobcov je enormný tlak udržiavať vysoké technologické štandardy. Popri tom však dostatočne nemyslia na bezpečnosť. Preto vznikajú zraniteľnosti, teda slabé miesta softvéru (systému alebo služby), ktoré môže útočník zneužiť a využiť ich pre svoj prospech.

Riešenia/Opatrenia:

- pravidelná aktualizácia všetkých prvkov – sieťové zariadenia, servery, koncové stanice, operačné systémy, softvér...
- sledovanie hrozieb a zraniteľností,
- dobrá politika aktualizácií,
- vyradovanie zastaranej technológie,
- monitoring,
- iné technické opatrenia.

Príklady

- zneužívanie zraniteľností v známych produktoch, používaných vo významných organizáciách,
- úniky údajov, penetrácia systému, dlhodobé špehovanie,
- zraniteľnosti v softvérových knižniciach, ktoré sú používané v ďalších produktoch, preto je náročné ich aktualizovať (nestačí aktualizovať knižnicu, každý výrobca čo ju používa, musí aktualizovať svoj produkt),
- 0-day zraniteľnosti – zraniteľnosti nulového dňa, o ktorých nevie výrobca a nie sú opravené – útočník ich môže využiť na širokú škálu útokov bez detekcie.



Typ útoku : **ZNESPRÍSTUPNENIE SLUŽBY**

Popis: Útoky na dostupnosť služby sú veľmi obľúbené medzi útočníkmi, nakoľko sú pomerne lacné a dokážu mať veľký efekt. Útok na dostupnosť služby znamená, že cieľom útočníka je znepriístupniť službu pre používateľov. Funkcionalita je tak obmedzená alebo úplne vyradená. Najčastejšie sa takýto typ útoku vykonáva na webové stránky alebo verejne dostupné služby. Existujú dva základné modely – DoS (Denial of Service), kde útočník využíva rôzne nástroje a amplifikačné mechanizmy, aby znepriístupnil službu a DDoS (Distributed Denial of Service) kde útočník typicky využíva viacero zariadení (napríklad v sieti botnet) na distribuovaný útok, ktorý má väčšiu silu.

Riešenia/Opatrenia:

- mať záložné lokality systémov a služieb, resp. ich redundanciu,
- publikácia statických webových stránok (redakčný systém, inštalovaný vo vnútornej sieti neprístupnej z Internetu, vygeneruje HTML súbory, obrázky a štýly, ktoré sú následne prenesené na hostingovú službu),
- oddelenie citlivých údajov a prevádzkovo kritických aktív od verejných webových stránok,
- používať služby na DDoS ochranu na rôznych úrovniach,
- implementácia bezpečnostnej infraštruktúry, ktorá vie filtrovať IP adresy útočníka vo veľkom objeme,
- implementácia webového aplikačného firewallu,
- využívanie Content Delivery Network na prevádzku webových služieb.

Príklady:

- DDoS útoky na webové stránky ministerstiev a iných štátnych organizácií počas vojny Ruska proti Ukrajine – aj v SR, ale aj v členských štátoch EÚ a NATO (vždy po nejakom vyhlásení alebo darovaní pomoci),
- DDoS útoky na webové stránky dôležitých organizácií (napr. banky alebo letiská), ale aj súkromných spoločností počas vojny na Ukrajine,
- výpadky služieb a ich nedostupnosť z dôvodu konfiguračnej chyby, poškodeného zariadenia alebo zlého škálovania.

Kybernetické útoky na Ukrajinu

Tri dni pred referendom o štatúte Krymu (13. marca 2014) odštartovalo Rusko 8-minútový DDoS útok zameraný na počítačové siete a komunikáciu. Mal odvrátiť pozornosť verejnosti od prítomnosti ruských vojsk na Kryme.

Onedlho zaútočili opäť. Malvér BlackEnergy, ktorý sa šíril cez phishingové e-maily, vyradil počas zimy 2015 kúrenie. Útok sa dotkol státisícov ľudí a naštrobil ich dôveru v štát a dodávateľov tepla. Zároveň ukázal, akú škodu vie napáchať kybernetický útok zacielený na kritickú infraštruktúru.

Proruská hackerská skupina uskutočnila sériu kybernetických útokov aj pred prezidentskými voľbami v máji 2014. Hackerská skupina CyberBerkut napadla sieť a vymazala súbory – snažila sa tak zmeniť výsledky volieb.

Kybernetické útoky smerované na Ukrajinu sa zintenzívnili v rokoch 2016 až 2021. Najznámejší z nich zahŕňal spustenie malvéru NotPetya. Tento útok sa považuje za najničivejší kybernetický útok v histórii. Šíril sa v roku 2017 cez účtovný softvér. NotPetya zasiahol jadrovú elektrárňu Černobyľ a približne 13-tisíc zariadení, ktoré používali verejné inštitúcie, banky, poštové služby, novinári, ale aj dopravná infraštruktúra a podniky. Počítačové disky boli zničené, čo znemožnilo obnovu údajov po zašifrovaní vírusom.

Aj Poľsko, Litva a Estónsko je podľa expertov spoločne s ďalšími krajinami regiónu najviac ohrozené veľkými kybernetickými útokmi. Avšak doteraz nebol žiadny z nich úspešný.

Výrazné škody však podnietili medzi odborníkmi na kybernetickú bezpečnosť a vládou rozsiahle úsilie zamerať sa dôkladnejšie na túto operačnú doménu. Investovalo sa do vzdelávania, prevencie, detekcie a riešenia kybernetických bezpečnostných incidentov.

Ruskí hackeri zaútočili aj na Slovenskú republiku

Hackeri z **Anonymous RU** zhodili v januári 2023 niekoľko slovenských webových stránok. V tom čase hackeri útočili na viacero štátnych webov vrátane stránok súkromných spoločností ako boli napríklad banky či spravodajské weby. Nefunkčné boli napríklad stránky NR SR, MV SR, MO SR, Prima banky, Privat banky a ďalšie. No zdá sa, že nakoniec sme predsa len padli proruským hackerským skupinám do hľadáča znova.

Ruská hackerská skupina **Anonymous RU** na sociálnej sieti Telegram oznámila, že začala útočiť na prvé slovenské ciele. Rovnako nám poslali strohé varovanie.

„Vydávame varovanie Slovenskej republike za podporu banderovských úradov na Ukrajine a presun MIG-29!“, hovoria ruskí Anonymous.

Spolu s varovaním vyššie zdieľali aj prvé internetové stránky, ktoré znefunkčnili. Išlo o web NR SR, NBS a Ministerstva obrany, Exim banky či JT banky. Všetky stránky boli nedostupné.

Tento útok prišiel krátko potom, ako Slovensko poslalo na Ukrajinu prvé stíhačky a ďalšie vojenské vybavenie, ktoré má pomôcť Ukrajincom v bojoch proti okupantom.

Z príspevku hackerov je zrejmé, že kybernetický útok súvisí s pomocou Kyjevu.

Išlo útok typu DDos. Pre tento typ útoku je typické, že útočník pošle tak veľký počet požiadaviek na server, až ľudovo povedané, spadne. Následkom toho je, že webové stránky a internetové služby nefungujú.

6. Platforma TikTok zábava alebo hybridná hrozba

TikTok – sociálna sieť: Súkromné dáta sa dajú predat tretím stranám (napr. na spearphishing a vydieranie) a informácie o vašom správaní v kybernetickom priestore môžu byť zneužitú na adresnú politickú kampaň financovanú škodlivými aktérmi, ktorej cieľom môže byť aj destabilizácia demokratického systému. Všetky videá je možné po natočení modifikovať prostredníctvom rôznych grafických alebo hudobných efektov a filtrov. Práve jednoduchosť používania a popularita tejto formy rýchlo a jednoducho pochopiteľného obsahu podporila vznik mnohých extrémnych a často nebezpečných výziev (často nebezpečné aktivity, ktoré užívatelia následne zdieľajú na platforme), ale aj mladých úspešných názorových opinion lídrov (mienkotvorných osôb) (ang. opinion leader) a influencerov.

Kybernetická bezpečnosť TikTok: v

- v aplikácii pre iOS spočívala existencia zabudovaného šifrovacieho kľúča a umožňovala odšifrovať dáta hocikomu, kto získal ku kľúču prístup,
- aplikácie nemali zašifrovaný presun obrázkov videí a lajkov (označení páči sa mi), čo umožňovalo útočníkovi, prostredníctvom sledovania sieťovej prevádzky vykonávať extrakciu osobných a iných citlivých údajov (zraniteľnosť popísaná a testovaná inými bezpečnostnými výskumníkmi,
- zraniteľnosť typu SMS spoofing. Zraniteľnosť umožňuje zaslať SMS správu, ktorá bude v zariadení prijímateľa zobrazená ako odoslaná priamo od organizácie vlastniacej TikTok. Zraniteľnosť by sa dala použiť na ďalšie útoky, pri ktorých útočník potrebuje, aby obeť klikla na URL adresu, napr. phishingové kampane,
- zraniteľnosť je podmienená zapnutou aplikáciou, ktorej stačí fungovať v minimalizovanom móde a jej možné zneužitie je alarmujúce. Aplikácie sa tak dokážu dostať nie len ku všetkým heslám kopírovaným z bezpečnostných aplikácií, ale aj ku aktuálnej polohe zariadenia, ktorá je súčasťou interných informácií kopírovaných fotografií,
- TikTok cez HTTP presúva videá, profilové fotografie aj vzorky videí (preview). Tento nešifrovaný prenos dát umožňuje bez problémov zbierať tieto dáta vlastníkom verejných WIFI, internetovým poskytovateľom aj spravodajským agentúram. Aplikáciu to robí zraniteľnou aj voči MITM útokom (man-in-the-middle), ktoré by umožnili vymeniť video alebo obrázok uploadovaný z populárneho TikTok účtu za úplne iné video. Útočník by tak obeť mohol podvrhnúť škodlivý obsah, ktorý by sa javil ako vierohodný.

Súkromie a bezpečnosť používateľských dát v Číne: Cieľom aktivity je poskytnutie prístupu čínskej komunistickej vlády ku všetkým dátam zahraničných firiem podnikajúcich na území Číny. Takto získané údaje môžu následne čínski predstavitelia (spravodajské služby a armáda) zdieľať so štátnymi firmami, a tak nad zahraničnými firmami obchodujúcimi na území Číny získajú kompetitívnu výhodu. Poskytovanie informácií bolo do vydania kryptografického zákona na vyžiadanie, avšak v súčasnosti čínska vláda získava dáta zo serverov invazívnym spôsobom – požaduje do ukladaných dát priamy prístup a obchodné tajomstvo nie je rešpektované.

TikTok zbiera nasledovné používateľské dáta:

- dáta o lokácii: informácie o lokácii vrátane lokačných informácií na základe simkarty/IP adresy, GPS súradnice s povolením od používateľa.
- informácie o zariadení: model zariadenia, poskytovateľ telekomunikačných služieb, nastavenie času, operačný systém,
- názvy aplikácií, súborov a ich typy, vzory a rytmy písania, metadáta, históriu navštívených stránok, históriu vyhľadávania, cookies.

Dáta používa na:

- cielená reklama,
- použitie obsahu používateľov na marketing platformy,
- dedukciu ďalších informácií: vek, pohlavie, záujmy,
- detekcie obťažovania, podvodov a ilegálnych aktivít,
- ostatné účely, o ktorých bude v danú dobu používateľ notifikovaný.

Spoločnosť TikTok informuje, že nepredáva osobné informácie tretím stranám. Zdieľa ich však s poskytovateľmi služieb a so svojimi partnermi. Informácie môže zdieľať s materskou spoločnosťou, dcérskou spoločnosťou alebo inou pridruženou spoločnosťou ich firemnej skupiny. V prípade významnejších problémov spoločnosť informácie zdieľa v súvislosti s „významnými podnikovými transakciami“, napr. predaj webovej stránky, fúzia, predaj majetku alebo v prípade bankrotu.

Platí známe pravidlo, že ak si neplatím za produkt, produktom som sám. Všetky veľké a populárne sociálne siete ako Facebook, Instagram, Snapchat, Youtube či práve TikTok predávajú informácie a údaje o používateľoch a ich návykoch iným spoločnostiam, ktoré cez ne cielene „marketujú“ svoje produkty na presne vybraného človeka. Práve na základe poznania jeho osobnosti a preferencií.

TikTok vďaka nepretržitému zberu údajov pozná správanie používateľa v aplikácii. Na základe prezeraného obsahu, lajkov či času, ktorý strávi sledovaním jednotlivých videí, dokáže vytvoriť relatívne presný psychologický profil alebo typ osobnosti daného užívateľa. To ani nehovorím o všetkých dátach, ktoré možno zbiera v mobile. Na základe toho vie v budúcnosti pripraviť cielenú, **na mieru šitú politickú kampaň či propagandu s dosahom na miliardy ľudí** s cieľom promovovať napríklad záujmy Číny alebo potlačiť záujmy západného sveta.

TikTok sa dá použiť ako spyware, špehovací nástroj. Aplikácia dokáže využiť slabiny telefónu, eskalovať privilégiá, získavať ďalšie povolenia a istým spôsobom nad ním získať kontrolu a zbierať informácie o používateľovi. Ďalší dôvod je, že vlády chcú mať kontrolu nad online obsahom.

Pri návšteve Číny si musíte na hraniciach nainštalovať do telefónu štátnu aplikáciu, ktorá počas celého pobytu monitoruje vaše aktivity. Na základe rôznych parametrov vám zvyšuje alebo znižuje tzv. sociálne skóre, ktoré má aj každý obyvateľ krajiny.

NCKB SK-CERT v súvislosti s používaním TikTok všeobecne odporúča

- v online komunikácii dodržiavať všetky pravidlá kybernetickej hygieny,
- dôkladne čítať, aké povolenia si aplikácia vyžaduje a zodpovedať si nasledovné otázky:
 - sú v zariadení **citlivé údaje**, ktoré nechcem, aby mal výrobca aplikácie k dispozícii ?
 - **potrebuje** aplikácia tieto prístupy na svoju bežnú funkciu ?
 - má aplikácia **alternatívu**, ktorá si nevyžaduje takéto povolenia na jej fungovanie ?
- do doby, kým nedôjde k úprave podmienok ochrany osobných údajov a k transparentnej reakcii TikTok na obvinenia, **aplikáciu odporúčame odstrániť zo zariadenia/neinštalovať ju**,
- zamestnancom **verejnej správy** a všeobecne zamestnancom poskytovateľov základných služieb podľa zákona o kybernetickej bezpečnosti **neodporúčame inštalovať aplikáciu TikTok**,
- aplikácia TikTok je v celej infraštruktúre Kancelárie Národnej rady (NR) SR **blokována a nebude možné ju používať.**,
- inštalujte len aplikácie, ktoré sú vyvíjané mimo čínskeho trhu,
- používajte hardvér, ktorého výrobcu nie je spoločnosť spadajúca pod čínske právo.

Ak však chcete aplikáciu TikTok naďalej používať (NCKB SK-CERT)

- používať aplikáciu TikTok na inom zariadení než na tom, ktoré používate na bežné aktivity, iné sociálne siete a na pracovné účely,
- pri vytváraní účtu na sociálnej sieti TikTok **nepoužívať** na prihlásenie **účet na inej sociálnej sieti**, spoločnosť tak získa veľké množstvo ďalších súkromných dát,
- zamestnancom **verejnej správy** a poskytovateľom základných služieb, ktorý chcú využívať TikTok na marketingové/iné účely neodporúčame inštalovať TikTok na zariadenia s prístupom ku služobným emailom a súborom súvisiacim s výkonom zamestnania,
- ku všetkým informáciám, ktoré na sociálnej sieti TikTok získate je nutné **byť skeptický** a riadiť sa všeobecnými zásadami:
 - čím je informácia závažnejšia a **extrémnejšia**, tým je **podozrivejšia**,
 - „extrémne obvinenia si vyžadujú extrémne dôkazy,“
 - to, že bola informácia zdieľaná z dôveryhodného zdroja, neznamená, že bola nahraná dôveryhodnou osobou,
 - každú podozrivú informáciu je nutné **overiť z viacerých zdrojov**.

7. Príklad hybridnej hrozby použitím špionážneho softvéru „PEGASUS“ a reakcia EÚ

Pegasus je nástroj na vzdialený prístup s funkciami spywaru. Jeho varianty pre Android dokážu extrahovať údaje z často používaných chatovacích aplikácií ako sú WhatsApp, Facebook Messenger a Viber, alebo z e-mailových klientov a prehliadačov.

Špionážny softvér môže sledovať nič netušiacich používateľov na diaľku prostredníctvom na diaľku zapnutého mikrofónu a kamery telefónu a môže tiež snímať snímky obrazovky alebo zaznamenávať text písaný na klávesnici. Tieto vlastnosti z neho robia veľmi nebezpečný nástroj.

Pegasus je vyvinutý izraelskou spoločnosťou s názvom NSO. Keď tento softvér prenikne do telefónu, začne extrahovať údaje z telefónu používateľa. Číta texty, správy, kontaktné údaje, nahráva hlas a hovory. Dokáže dokonca ovládať kameru a sledovať GPS polohu používateľa.

Novinári na celom svete čelia hrozbe už pomerne známeho špionážneho softvéru Pegasus. Vytvára ho izraelská spoločnosť NSO Group, ktorá ho potom predáva autoritárskym vládam ale aj súkromným spoločnostiam. Podľa uniknutých údajov ho tieto vlády použili na monitorovanie mobilných telefónov približne 180 novinárov zo známych svetových médií a tlačových agentúr, ako sú The Wall Street Journal, CNN, Rádio Slobodná Európa, The New York Times, Le Monde, AFP, Reuters, Bloomberg a ďalšie.

Expert hovorí, že je zložité zistiť, či je v telefóne nainštalovaný Pegasus alebo nie. Používatelia dostanú jeden hovor WhatsApp a bez ohľadu na to, či hovor prijmú alebo neodpovedia, softvér sa nainštaluje do telefónu.

Európsky parlament zriadil výbor „PEGA“

Dňa 10. marca 2022 sa EP rozhodol zriaďiť výbor **PEGA** na vyšetrenie údajného porušenia alebo nesprávneho úradného postupu pri uplatňovaní práva EÚ v súvislosti s používaním programu Pegasus a ekvivalentného softvéru na sledovanie spywaru.

Výbor **PEGA** po ročnom skúmaní situácie v tejto oblasti prijal záverečnú správu a odporúčania pre inštitúcie EÚ a členské krajiny eurobloku. *„Nezákonné sledovanie politických oponentov, novinárov, právnikov a ľudskoprávných aktivistov je proti základným hodnotám Európskej únie a nesmie sa používať ako politická zbraň.“* EP nevidí cestu v tom, aby špionážne softvéry (spywary) ako Pegasus či Predátor boli zakázané. Členské krajiny EÚ potrebujú pokročilé technologické nástroje, aby mohli brániť národnú bezpečnosť a čeliť hrozbám akými sú terorizmus, organizovaný zločin alebo útoky proti ústavnému poriadku. *„Je však kľúčové, aby sa tak dialo v jasne určených hraniciach“*.

Zneužívanie spywaru v Poľsku a Maďarsku, na čo poukázalo vyšetrenie PEGA, bolo „zjavným porušením zásad právneho štátu“. Podľa EPP existuje riziko, že súčasná poľská vláda by mohla opäť špehovať opozíciu alebo novinárov pred parlamentnými voľbami na jeseň tohto roku. *„Sme znepokojení možnosťou, že by vláda PiS mohla opäť zasahovať do nadchádzajúcich poľských parlamentných volieb pomocou spywaru,“* opísal situáciu španielsky europoslanec Juan Ignacio Zoido, hovorca skupiny EPP vo vyšetrovacom výbore **PEGA**.

8. Blíži sa ďalšia úroveň umelej inteligencie „AI“ a naša demokracia nie je pripravená

Sociálne médiá už vyradili pilier spod našich demokratických inštitúcií tým, že ľuďom s extrémnymi názormi uľahčili spojenie a koordináciu a teraz prichádza AI. Zoznam aktivít, o ktorých OpenAI vie, že ich technológia môže umožniť a ktoré preto zakazuje vo svojich zásadách používania:

- Nelegálna činnosť.
- Materiál zameraný na sexuálne zneužívanie detí.
- Generovanie nenávistného, obťažujúceho alebo násilného obsahu.
- Generovanie malvéru.
- Činnosť, ktorá má vysoké riziko fyzického zranenia, vrátane: vývoja zbraní; vojenstvo a vedenie vojny; riadenie alebo prevádzka kritickej infraštruktúry v energetike, doprave a vode; obsah, ktorý propaguje, povzbudzuje alebo zobrazuje činy sebapoškodzovania.
- Činnosť, ktorá predstavuje vysoké riziko ekonomickej škody, vrátane: viacúrovňového marketingu, hazardných hier, pôžičiek pred výplatou, automatizovaného určovania oprávnenosti na získanie úveru, zamestnania, vzdelávacích inštitúcií alebo verejných asistenčných služieb.
- Podvodná alebo klamlivá činnosť vrátane: podvodov, koordinovaného neautentického správania, plagiátorstva, astroturfingu, dezinformácií, pseudofarmaceutík.
- Politická kampaň alebo lobing vytváraním veľkého množstva materiálov na kampaň.
- Činnosti, ktoré porušujú súkromie. Neoprávnené vykonávanie právnej alebo lekárskej praxe alebo poskytovanie finančného poradenstva.

Príklad účelového videa vysielaného v sieti „Telegram“

Dňa 16. marca 2022 ukrajinský televízny kanál Ukrajina 24 bol hacknutý proruskými hackermi, čo viedlo k vysielaniu správy údajne od prezidenta Zelenského vyzývajúceho ukrajinských vojakov, aby sa vzdali.

S očakávaným vývojom na báze AI technológií a ich dostupnosti pre verejnosť, je sofistikovanosť týchto operácií v tom že ukrajinskí vojaci sa mali zdať ruským silám. Toto falošné video bolo tiež zverejnené na viacerých platformách sociálnych médií, vrátane ruského „VKontakte“ ktorý je pod nepriamym dohľadom Kremľa. Falfifikát bol rýchlo odhalený a nemal žiadny dopad na ukrajinské obyvateľstvo.

Napriek tomu použitie týchto technológií v čase vojny je nová vec - operácie vplyvu v kombinácii s simultánnou akciou v kyberpriestore na hacknutie TV kanálu „Ukrajina 24“. Čo sa týka hybridnej vojny, kombinácia operácií v kybernetickej oblasti a informácií domén je v súlade s ruským habitusom alebo podvodom.

Klamanie vo vojenskom zmysle je definované v spoločnej publikácii amerického ministerstva obrany 3-13.4 ako „akcie vykonávané s cieľom zámerne uviesť do omylu protivníkov vo vojenských, polovojenských alebo násilných extrémistických organizáciách s rozhodovacími právomocami, čím spôsobí, že protivník podnikne konkrétne kroky (alebo nečinnosť), ktoré prispievajú k dosiahnutiu cieľa“.

POZOR: Nízka úroveň digitálnej gramotnosti a povedomie o mediálnom falšovaní by mohlo viesť k rôznym dopadom v reálnom živote, ako sú napríklad protesty alebo dokonca nepokoje.

STUXNET – prvá kybernetická zbraň na svete, ktorá ovplyvnila fyzickú infraštruktúru

Stuxnet sa zameriaval na iránske jadrové centrifúgy, poškodil a zničil kritické vojenské kapacity a spôsobil veľké narušenie iránskeho jadrového programu (vývoj USA + Izrael). Po infiltrácii do iránskeho zariadenia na obohacovanie jadrových zbraní **Stuxnet** začal hľadať počítače pripojené k programovateľným logickým ovládačom (PLC), ktoré interagujú a riadia centrifúgy a iné priemyselné stroje zapojené do výroby jadrového materiálu na zbrane. Červ potom zmenil kód PLC tak, aby sa **centrifúgy otáčali príliš rýchlo** a príliš dlho, pričom zároveň odosielať falošné údaje, aby sa zdalo, že všetko funguje normálne. To spôsobilo veľké poškodenie citlivých nástrojov a dočasne **vykoľajilo iránsky jadrový program**.

Keďže cieľové jadrové zariadenie nebolo pripojené k internetu, vírus **Stuxnet** nebolo možné doručiť digitálnym hackom. Namiesto toho bol červ zrejme doručený cez laptop, USB kľúč alebo iné vymeniteľné médium. Len čo bol infikovaný jeden počítač, červ sa rýchlo replikoval a skákal zo zariadenia na zariadenie, kým nebola ohrozená celá sieť.

Hoci bol vírus **Stuxnet** navrhnutý tak, aby vypršal v roku 2012, po úniku mimo pôvodne cieľových zariadení, mačka bola dobre a naozaj mimo. Odvtedy došlo k množstvu ďalších kybernetických útokov na infraštruktúru pomocou červov s podobnými vlastnosťami a schopnosťami ako Stuxnet.

Prehľad najvýznamnejších spin-offs - Stuxnet

Duqu

V roku 2011 analytici hrozieb objavili nového červa a nazvali ho Duqu. Nápadné podobnosti medzi Duqu a Stuxnet viedli odborníkov k presvedčeniu, že tieto dva kmene malvéru spolu úzko súvisia. V skutočnosti boli *takmer identické* – jediný rozdiel bol v tom, že Duqu nebol navrhnutý tak, aby sabotoval stroje, ale aby pôsobil ako spyware tým, že zachytával stlačenia klávesov a zbieral systémové údaje.

Flame

V roku 2012 sa objavilo viac malvéru u ktorého existuje podozrenie, že je prepojený so Stuxnetom. Vedci, ktorí nazvali novú hrozbu Flame, zistili, že vírus zdieľa veľkú časť svojho kódu so Stuxnetom, najmä spôsob, akým bol navrhnutý tak, aby sa zameriaval na rovnaké zraniteľnosti systému Windows a šíril sa prostredníctvom úložné zariadenia USB.

Petya

Hoci to priamo nesúvisí so Stuxnetom, malvér Petya , ktorý v roku 2017 pustošil inštitúcie na Ukrajine, je ďalším príkladom toho, ako sa kybernetické útoky čoraz viac stávajú zbraňami proti celým sektorom a dokonca aj krajinám. Hoci je Petya klasifikovaná ako ransomvér, zdá sa, že hlavným cieľom Petvy bolo spôsobiť chaos v ukrajinskom bankovom systéme.

Snake

Najsofistikovanejší malvér, na ktorý sa ruská vláda spoliehala pri špionážnych kampaniach. Ide o krádeže dokumentov zo stoviek počítačových systémov patriacich vládam členov NATO

Kybernetické útoky ako vplyvové operácie v kontexte amerických volieb v roku 2016

Z hľadiska informačných operácií sú nezanedbateľné aj pokusy Kremľa o ovplyvnenie výsledku volieb vo viacerých krajinách vo svoj prospech. Najlepšie zdokumentovaným príkladom takýchto snáh sú prezidentské voľby v USA v roku 2016. Hackeri vtedy získali a následne zverejnili údaje kompromitujúce demokratickú kandidátku Hillary Clinton. Vo veľkom sa angažovala aj IRA a ruské štátne médiá.

Počas volieb v roku 2016 na Facebooku prebiehali dve samostatné ruské kampane. Prvá prišla od ruskej vojenskej spravodajskej agentúry GRU. Spoločnosť Facebook prvýkrát objavila jej aktivitu v marci 2016, kedy agenti GRU vytvorili falošné účty a stránky, pomocou ktorých šíрили dezinformácie a falošné správy. Facebook zistil, že stránka prevádzkovaná Ruskom, známa ako DCLeaks, distribuuje novinárom ukradnuté e-maily z kampane demokratickej kandidátky Hillary Clinton. Spoločnosť však pôvodne nepodnikla nijaké kroky. Až keď sa zistilo, že dokumenty obsahujú osobné informácie, čo je zjavné porušenie pravidiel Facebooku, bola stránka DCLeaks zakázaná.

Zatiaľ čo Facebook zvažoval, čo urobiť s ruskou kampaňou hack-and-leak, Agentúra pre výskum internetu (Internet Research Agency, IRA) podnikla ďalšie operácie zasahujúce do volieb a politických procesov. Zistilo sa to až po voľbách v roku 2017, keď na to upozornil jeden z amerických senátorov. Následné vyšetrovanie ukázalo, že IRA zverejnila 80-tisíc príspevkov, zaplatila 100-tisíc dolárov za 3 300 reklám a oslovila až 126 miliónov Američanov.

Kybernetické útoky ako vplyvové operácie v kontexte volieb vo Francúzku v roku 2017

Kremeľ pravdepodobne zasahoval aj do volieb vo Francúzsku. Hackeri sa nabúrili minimálne do piatich účtov blízkych spolupracovníkov vtedy ešte prezidentského kandidáta Emmanuela Macrona a ukradli 15 GB dát, vrátane viac ako 21-tisíc e-mailov. Zverejnili ich dva dni pred druhým kolom volieb. Dve hodiny pred záverečnou televíznou debatou medzi Macronom a Marine Le Pen sa medzi ľuďmi rozšírila fáma „MacronGate“, podľa ktorej mal Macron tajný zahraničný účet. Tesne pred voľbami bol únik propagovaný trollmi a falošnými účtami na Twitteri. Takýchto tweetov sa objavilo za 24 hodín takmer pol milióna. Francúzsko síce oficiálne neprisúdilo túto operáciu Rusku, urobilo tak však niekoľko firiem v oblasti kybernetickej bezpečnosti, podľa ktorých sa malo jednať o skupinu APT28.

Skupinu hakerov experti pomenovali Pawn Storm (Útok pešiakom), známu skôr pod názvami Fancy Bear, APT 28 či Sofacy Group a Strontium. Teda mená, ktoré figurovali v útokoch na stranu Hillary Clintonovej. Nebolo by to prvý raz, keď ruskí hakeri figurujú ako podozriví. V minulosti ich napríklad obvinili z útoku na francúzsku televíziu TV5. Počas francúzskej kampane bolo na prvý pohľad jasné, koho preferujú prokremeľské stránky ako RT či Sputnik financované ruským štátom, a to aj v regióne strednej Európy. „Nielenže prevyšovala svojich oponentov v počte článkov, kde sa o nej hovorilo, ale dezinformačné stránky v strednej Európe ju len sťažka opisovali negatívnym spôsobom,“ napísal Globsec Policy Institute. Napríklad český Sputnik sa venoval Le Penovej 17-krát viac ako víťazovi prvého kola prezidentských volieb Macronovi, ktorý často od proputinovských stránok dostával nálepku „Rothschildovský kandidát“.

Zvýšené riziko kybernetických a bezpečnostných incidentov a iných škodlivých aktivít v súvislosti s voľbami v Slovenskej republike 2023

PHISHING A KOMPROMITÁCIA E-MAILOV

NBÚ očakáva, že útočníci budú využívať sociálne inžinierstvo najmä vo phishingových kampaniach (e-mailové, telefonické aj SMS). Zneužívaním témy volieb môžu viesť k neoprávnenému získaniu prístupu do e-mailových účtov alebo k získaniu iných citlivých údajov a ich následnému zneužitiu, napr. s cieľom zdiskreditovať osobu s významným spoločenským postavením, k získaniu prihlasovacích údajov do internetbankingu a následným okradnutím obete a pod.

DDOS ÚTOKY

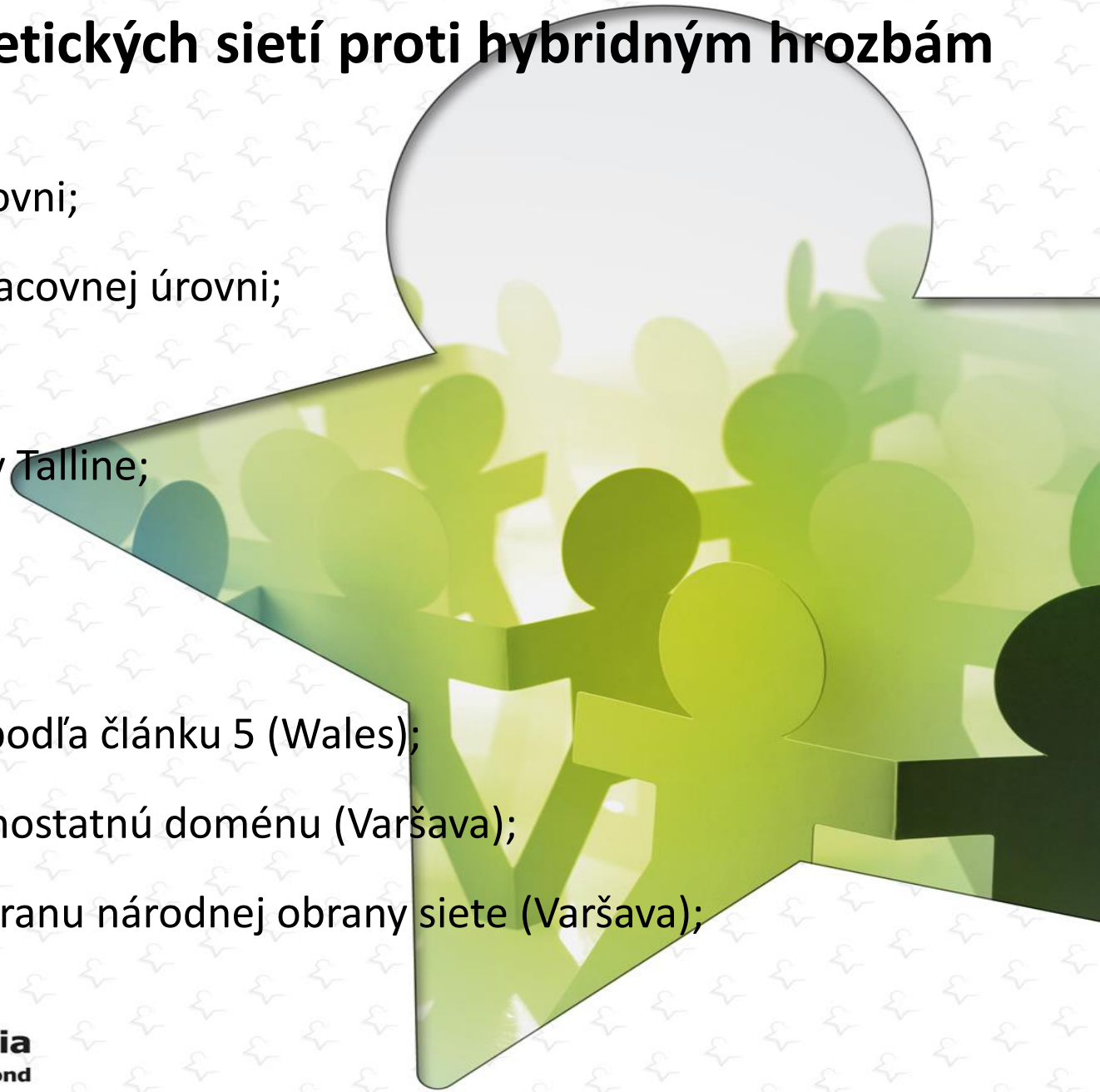
Očakávame kybernetické útoky proruský orientovaných hackerských skupín na slovenské ciele vo vzťahu k zabezpečeniu sietí a informačných systémov prevádzkovateľov základných služieb vrátane prvkov kritickej infraštruktúry a osobitne vo volebnej infraštruktúre ako súčasť hybridného pôsobenia Ruskej federácie s cieľom ovplyvňovať volebný proces. Predpokladanou formou útokov sú najmä DDoS útoky, čo však nevylučuje aj vykonávanie iných typov útokov.

VIZUÁLNA A OBSAHOVÁ MANIPULÁCIA

Národný bezpečnostný úrad predpokladá výskyt rôznych vplyvových operácií najmä využívaním falošných účtov, ktoré publikovaním rôzneho obsahu alebo diskusnými príspevkami môžu ovplyvňovať verejnú mienku. Jedným z nových prostriedkov sú aj deepfake videá alebo iné formy šírenia dezinformácií vizuálnou formou aj s pomocou umelej inteligencie. Môže dôjsť navonok k vernému napodobneniu výzoru a hlasu verejne známej osoby, ktorá však sprostredkuje falošný odkaz vytvorený útočníkom. Takéto deepfake videá môžu mať za cieľ zdiskreditovať osoby s významným postavením alebo zneužitím ich identity ovplyvňovať verejnú mienku pred a počas volieb. Rovnako môžu byť deepfake videá využité na rôzne podvodné aktivity.

9. Reakcia NATO na ochranu kybernetických sietí proti hybridným hrozbám

- výbor pre kybernetickú obranu na vysokej úrovni;
- Rada pre riadenie kybernetickej obrany na pracovnej úrovni;
- schopnosť reakcie na počítačové incidenty;
- centrum excelentnosti kybernetickej obrany v Talline;
- kybernetické partnerstvo NATO a priemyslu;
- politika rozšírenej kybernetickej obrany;
- kybernetické útoky môžu predstavovať útok podľa článku 5 (Wales);
- kybernetická obrana bude považovaná za samostatnú doménu (Varšava);
- národný záväzok kybernetickej obrany na ochranu národnej obrany siete (Varšava);



Bezpečnostná hrozba hybridných hrozieb v kybernetickom priestore

„Potenciálna príčina nechceného incidentu, ktorého výsledkom môže byť poškodenie systému alebo organizácie“

Bezpečnostné hrozby prírodného alebo ľudského pôvodu, môžu byť náhodné alebo úmyselné, z vnútra organizácie alebo mimo organizácie.

- ransomware,
- škodlivý softvér,
- hrozby sociálneho inžinierstva,
- hrozby voči údajom,
- hrozby proti dostupnosti: Denial of Service,
- Internetové hrozby,
- dezinformácie,
- útoky na dodávateľský reťazec.

- Konflikt medzi Ruskom a Ukrajinou zmenil podobu hrozieb. Nárasty hacktivistickej aktivity, kyberherci vykonávajúci operácie v súlade s kinetickou vojenskou akciou, mobilizácia hacktivistov.
- Geopolitika má naďalej silnejší vplyv na kybernetické operácie.
- Deštruktívne útoky sú významnou súčasťou operácií štátnych aktérov. Počas rusko-ukrajinského konfliktu, kybernetickí aktéri boli pozorovaní pri vykonávaní operácií v súlade s kinetickou vojenskou akciou.
- Nová vlna hacktivizmu bola pozorovaná najmä od začiatku rusko-ukrajinskej krízy.
- Dezinformácie sú nástrojom kybernetického boja. Používali sa ešte predtým, ako začala „fyzická“ vojna ako napríklad prípravná činnosť na ruskú inváziu na Ukrajinu.

Aké hybridné hrozby ohrozujú SR ?

Činnosť ruských spravodajských služieb

Na jar 2022 unikli nahrávky, na ktorých ruský vojenský pridelenec v SR verbuje, resp. odovzdáva finančnú čiastku za spoluprácu viacerým slovenským občanom. Vyhostovanie ruských spravodajských dôstojníkov operujúcich pod diplomatickým krytím a zníženie počtu zamestnancov na Veľvyslanectve Ruskej federácie v Bratislave dočasne utlmilo aktivity ruských spravodajských služieb v SR.

Čína

Vo vzťahu k SR posilňovali vplyv najmä na väzby v štátnych inštitúciách s cieľom využiť nadobudnuté kontakty na presadzovanie svojich politických a hospodárskych záujmov, šírenie čínskej propagandy či hospodársku špionáž.

Utečenecká vlna z Ukrajiny

Zneužitie voľnejšieho režimu na hraničných priechodoch SR s Ukrajinou štátnymi príslušníkmi tretích krajín nachádzajúcimi sa na území Ukrajiny na presun do EÚ vrátane rizikových osôb bez záznamu v príslušných policajných evidenciách.

PEX scéna na sociálnych sieťach

Trend šírenia akcelerationizmu bol v SR zaznamenaný v máji 2022 pri zadržaní občana SR, ktorý na sociálnej sieti Telegram verejne podnecoval k terorizmu a šíril návody na výrobu výbušnín. Prívržencom tohto hnutia bol aj útočník zo Zámockej ulice.

10. Bezpečnostné incidenty – NBÚ, CSIRT a SK-CERT

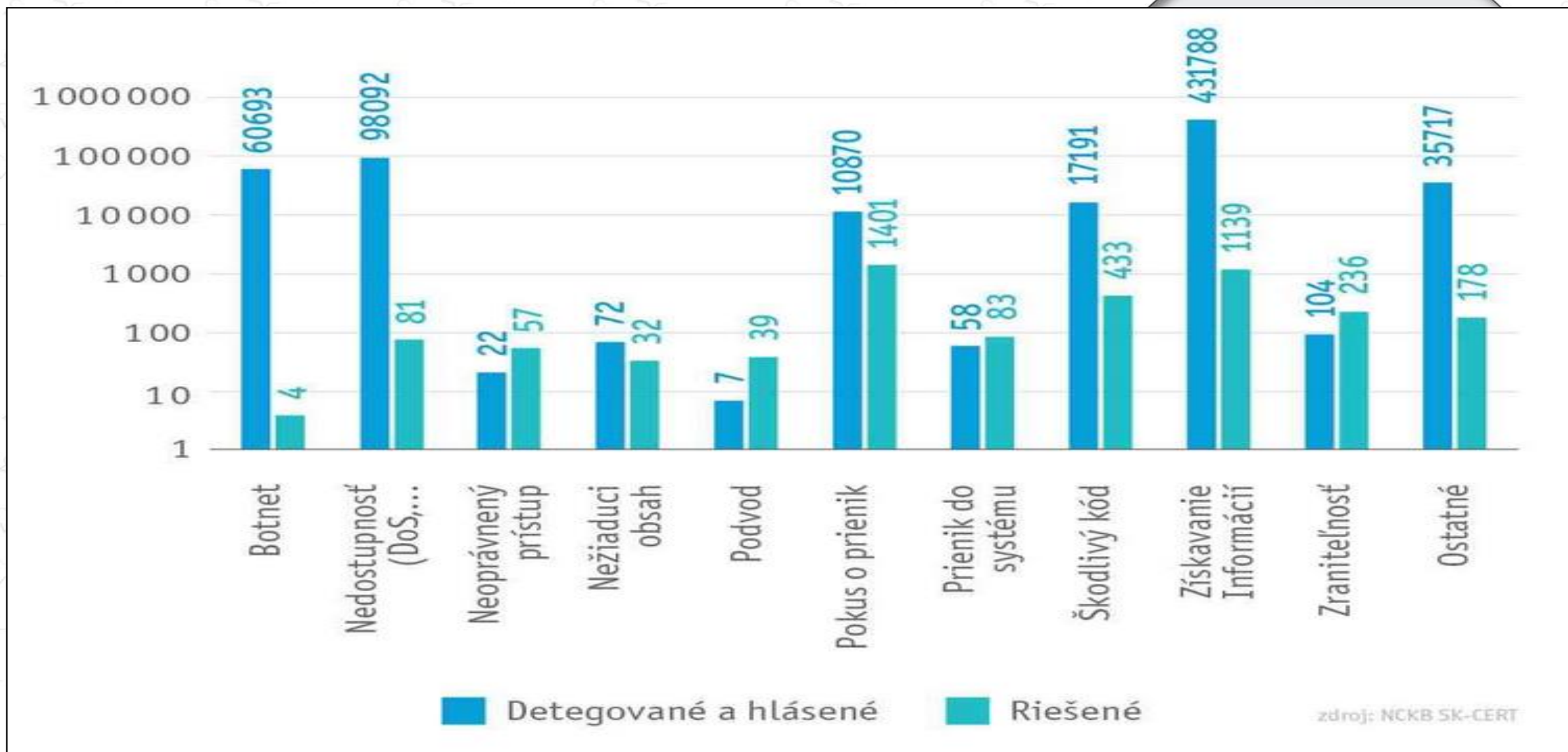
Kybernetickým bezpečnostným incidentom je akákoľvek udalosť, ktorá má z dôvodu narušenia bezpečnosti siete a informačného systému, alebo porušenia bezpečnostnej politiky alebo záväznej metodiky negatívny vplyv na kybernetickú bezpečnosť alebo ktorej následkom je :

- strata dôvernosti údajov, zničenie údajov alebo narušenie integrity systému,
- obmedzenie alebo odmietnutie dostupnosti základnej služby alebo digitálnej služby,
- vysoká pravdepodobnosť kompromitácie činností základnej služby alebo digitálnej služby,
- ohrozenie bezpečnosti informácií.

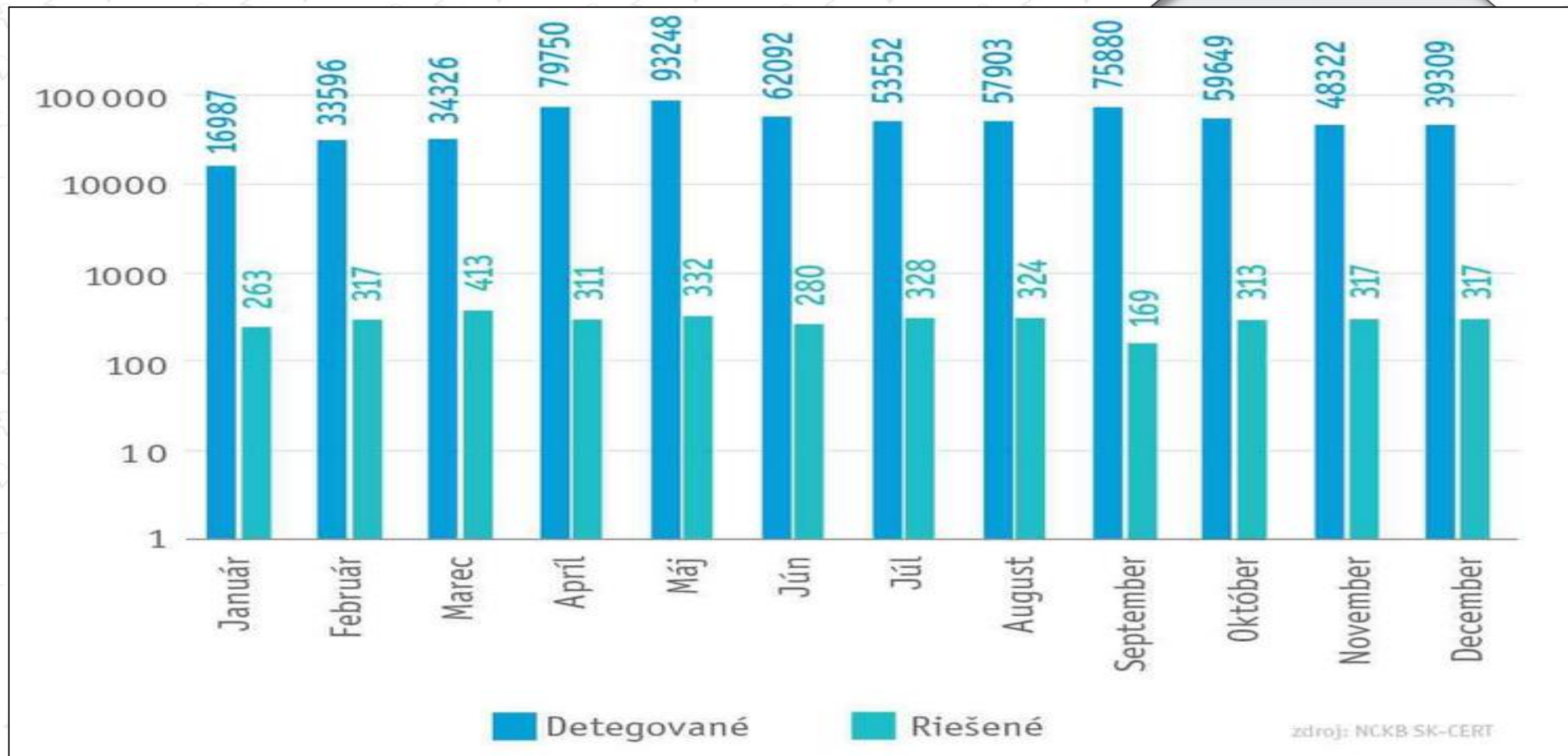
Najbežnejšími príkladmi bezpečnostných incidentov sú:

- preniknutie útočníka do systému,
- odopretie služby (anglicky Denial of service, „DoS“), prípadne špeciálny typ distribuovaného odopretia služby, kedy je útok realizovaný z mnohých IP adries (Distributed DoS, „DDoS“),
- prítomnosť škodlivého kódu,
- zlyhanie aplikácie kvôli chybe v kóde aplikácie,
- neúspešný pokus o prihlásenie sa do systému,
- odcudzenie, strata alebo poškodenie komponentov informačno-komunikačných technológií,
- odcudzenie, strata alebo poškodenie nosičov dát (notebooky, tablety, externé HDD, USB a podobne),
- odcudzenie, strata alebo poškodenie papierovej dokumentácie.

Počet detegovaných a hlásených a riešených incidentov podľa typu za rok 2021



Incidenty z časového hľadiska za rok 2021



Národný bezpečnostný úrad - v oblasti kybernetickej bezpečnosti

- riadi a koordinuje výkon štátnej správy,
- určuje štandardy, operačné postupy, vydáva metodiku a politiku správania sa v kybernetickom priestore,
- určuje zásady predchádzania kybernetickým bezpečnostným incidentom a zásady ich riešenia,
- vypracúva národnú stratégiu kybernetickej bezpečnosti a ročnú správu o stave kybernetickej bezpečnosti v Slovenskej republike v spolupráci s príslušnými štátnymi orgánmi,
- je národným kontaktným miestom pre kybernetickú bezpečnosť pre zahraničie a zabezpečuje spoluprácu s jednotnými kontaktnými miestami členských štátov Európskej únie a Organizácie Severoatlantickej zmluvy,
- plní notifikačné a nahlasovacie povinnosti voči príslušným orgánom Európskej únie a Organizácie Severoatlantickej zmluvy a podieľa sa a podporuje vytváranie partnerstiev na národnej a medzinárodnej úrovni v oblasti kybernetickej bezpečnosti,
- zabezpečuje členstvo Slovenskej republiky v skupine pre spoluprácu a v sieti jednotiek CSIRT,
- spolupracuje s ústrednými orgánmi, inými orgánmi štátnej správy a jednotkami CSIRT, prevádzkovateľmi základných služieb a poskytovateľmi digitálnych služieb pri plnení úloh podľa tohto zákona,
- spravuje a prevádzkuje jednotný informačný systém kybernetickej bezpečnosti,

Vládna jednotka pre riešenie počítačových incidentov v SR podľa zákona č.69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov zriadená ako organizačný útvar Ministerstva investícií, regionálneho rozvoja a informatizácie SR.

Zabezpečuje služby spojené so zvládaním bezpečnostných incidentov, odstraňovaním ich následkov a následnou obnovou činnosti informačných systémov a súvisiacich informačných a komunikačných technológií v rámci celej IT VS. Poskytuje aj služby preventívneho a vzdelávacieho charakteru.

K hlavným cieľom CSIRT.SK patrí:

1. Riešenie kybernetických bezpečnostných incidentov v spolupráci s vlastníkmi a prevádzkovateľmi postihnutých častí IT VS , telekomunikačnými operátormi, poskytovateľmi internetových služieb (ISP) a prípadne inými štátnymi orgánmi (napr. polícia, vyšetrovatelia, súdy).
2. Budovanie a rozširovanie povedomia verejnosti vo vybraných oblastiach informačnej, resp. kybernetickej bezpečnosti.
3. Kooperácia s partnerskými organizáciami a združeniami v oblasti kybernetickej bezpečnosti na národnej a medzinárodnej úrovni.

Služby

Služby pre klientov budú rozdelené na nasledujúce dve skupiny

Reaktívne služby:

1. riešenie incidentov,
2. varovania a upozornenia,
3. detekcia incidentov,
4. analýza incidentov,
5. ohraničenie, vyhladenie incidentu a obnova,
6. poskytnutie pomoci pri riešení incidentu na mieste,
7. reakcia na incidenty,
8. podpora pri riešení incidentov,
9. koordinácia činností pri reakcii na incidenty,
10. návrh opatrení na prevenciu ďalšieho pokračovania, šírenia a opakovania sa incidentov,
11. analýza škodlivého softvéru.

Proaktívne služby:

1. vzdelávanie a budovanie všeobecného povedomia v oblasti informačnej bezpečnosti,
2. odborné školenia a výcvik,
3. spolupráca s ostatnými jednotkami CSIRT,
4. monitorovanie a dokumentovanie incidentov,
5. pripojenie sa do jednotného systému kybernetickej bezpečnosti (JSKB),
6. prijímanie a zasielanie včasných varovaní o incidentoch cez (JSKB),
7. oznámenia o existujúcich zraniteľnostiach,
8. technologický dozor,
9. konfigurácia a údržba bezpečnostných nástrojov, aplikácií a infraštruktúry,
10. služby detekcie prienikov,
11. distribúcia informácií týkajúcich sa bezpečnosti,
12. monitorovanie stavu hrozieb v oblasti IKT,
13. vzdelávanie a budovanie bezpečnostného povedomia,
14. konzultačná činnosť v oblasti informačnej bezpečnosti,
15. audit informačnej bezpečnosti,
16. asistencia pri zakladaní nových jednotiek CSIRT.

Nahlásiť
incident

Nahlásiť
zraniteľnosť

Registrácia
Achilles

Aktuality

23. februára 2023

[Mesačná správa CSIRT.SK – Január 2023](#)

9. februára 2023

[Mesačný prehľad kritických zraniteľností január 2023](#)

20. januára 2023

[Mesačná správa CSIRT.SK – December 2022](#)

Oznámenia a varovania

23. februára 2023

[Kritická zraniteľnosť FortiNAC má exploit, FortiWeb možno onedlho](#)

23. februára 2023

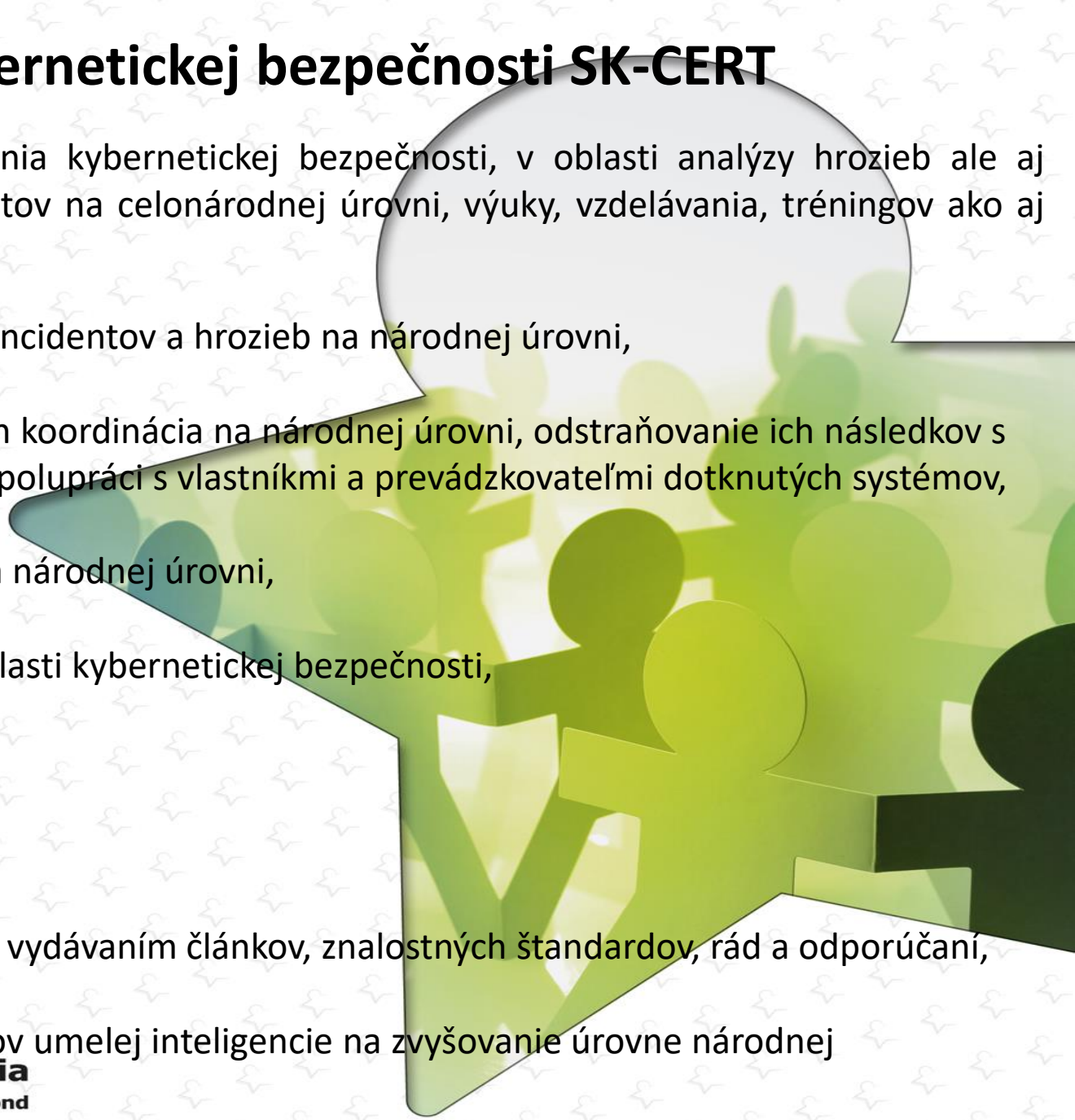
[Microsoft opravil tri závažné zero-day zraniteľnosti](#)

23. februára 2023

[Kritická zraniteľnosť ClamAV, Cisco](#)

Zabezpečuje národné a strategické aktivity v oblasti riadenia kybernetickej bezpečnosti, v oblasti analýzy hrozieb ale aj koordinácie riešenia kybernetických bezpečnostných incidentov na celonárodnej úrovni, výuky, vzdelávania, tréningov ako aj výskumu:

- sledovanie, detekcia a vyhodnocovanie kybernetických incidentov a hrozieb na národnej úrovni,
- riešenie kybernetických bezpečnostných incidentov a ich koordinácia na národnej úrovni, odstraňovanie ich následkov s následnou obnovou činnosti informačných systémov v spolupráci s vlastníkmi a prevádzkovateľmi dotknutých systémov,
- strategická analýza incidentov, zraniteľností a hrozieb na národnej úrovni,
- vytváranie podkladov pre strategické rozhodovanie v oblasti kybernetickej bezpečnosti,
- služby bezpečnostného a prevádzkového monitoringu,
- forenzná analýza, analýza malvéru,
- zvyšovanie kybernetického bezpečnostného povedomia vydávaním článkov, znalostných štandardov, rád a odporúčaní,
- aplikácia vytvorených inovatívnych techník a prostriedkov umelej inteligencie na zvyšovanie úrovne národnej kybernetickej bezpečnosti.



O NÁS

SLUŽBY

ŠTATISTIKY

PUBLIKÁCIE

RADY A NÁVODY

LEGISLATÍVA



VAROVANIE NBÚ

Varovanie pred zvýšeným rizikom kybernetických útokov

27. februára 2023

Národný bezpečnostný úrad vyhlasuje varovanie pred zvýšeným rizikom kybernetických bezpečnostných incidentov prorusky orientovaných komunitných hackerských skupín na slovenské ciele vo vzťahu k zabezpečeniu sietí a informačných systémov prevádzkovateľov základných služieb vrátane prvkov kritickej infraštruktúry a iných organizácií. Varovanie je platné od 28. februára do 2. marca 2023. Predpokladaným výkonom sú DDoS útoky na úrovni L7, čo však nevylučuje aj vykonávanie...



TL;DR: Pozor na útočné SMS! (8. týždeň)

24. februára 2023

Dva závažné kybernetické útoky začali SMS správou od útočníka a unikli dáta desiatok miliónov cestovateľov indických železníc. Kyberzločinci začali aktívne zneužívať tematiku chatbotov na to, aby zaujali potenciálne obete, ransomvérový gang zarába na poisťovniach a zaznamenané boli aj úspechy a jeden neúspech bezpečnostných zložiek. Podcenili vyšetровatelia problém? Zamestnanec hernej spoločnosti Activision sa stal cieľom SMS phishingového...

[čítať celý článok](#)

Aktuálne hrozby



SK-CERT Bezpečnostné varovanie V20230227-05

Dôležitosť Kritická Klasifikácia
Neutajované/TLP WHITE CVSS Skóre
9.8 Identifikátor PTC ThingWorx Edge
— ...

27. februára 2023



SK-CERT Bezpečnostné varovanie V20230227-04

Dôležitosť Kritická Klasifikácia
Neutajované/TLP WHITE CVSS Skóre
9.8 Identifikátor IBM Aspera Faspex —
...

27. februára 2023



SK-CERT Bezpečnostné varovanie V20230227-03

Dôležitosť Kritická Klasifikácia
Neutajované/TLP WHITE CVSS Skóre
9.8 Identifikátor Zyxel routre
LTE3316-M604 a ...

27. februára 2023

[všetky oznámenia](#)

Tweets by sk_cert

Čo robí štát pre elimináciu hybridných hrozieb ?

- doteraz bolo realizované zanedbateľné množstvo aktivít smerom k odbornému vzdelávaniu pracovníkov verejnej správy ale aj príslušníkov PZ v oblasti hybridných hrozieb,
- **Akčný plán koordinácie boja proti hybridným hrozbám (2022-2024),**
- **národná stratégia kybernetickej bezpečnosti na roky 2021 až 2025** – v ktorej jeden zo strategických cieľov je **VZDELÁVANIE**,
- akčný plán k tejto stratégii obsahuje v oblasti vzdelávania 55 úloh.

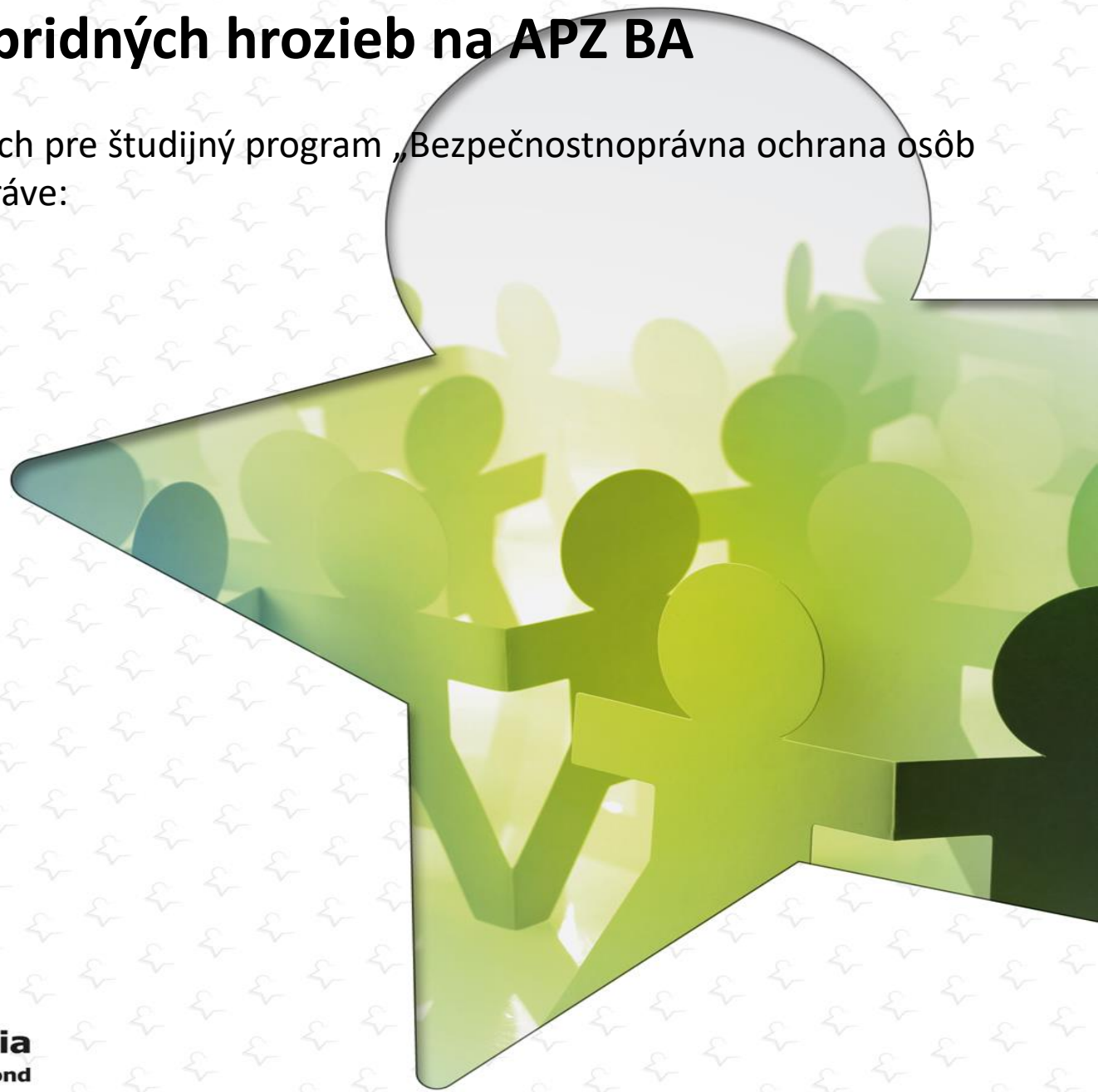
Nevyhnutnosťou je vypracovať koncepciu vzdelávania s rôznym profesným zameraním:

- odborníci v oblasti riešenia kybernetických bezpečnostných incidentov,
- forenzní špecialisti,
- vyšetrovatelia PZ a kriminalisti PZ so špecializáciou na „hybridné hrozby“,
- manažéri kybernetickej bezpečnosti,
- auditori kybernetickej bezpečnosti,
- strategická komunikácia v prípadoch hybridných hrozieb.

Vzdelávanie v oblasti hybridných hrozieb na APZ BA

Problematika „**Hybridné hrozby**“ v povinných predmetoch pre študijný program „Bezpečnostnoprávna ochrana osôb a majetku a bezpečnostnosprávne služby vo verejnej správe:

1. Informačný manažment.
2. Strategický manažment.
3. Krízový manažment.
4. Kriminológia 2.
5. Vyšetrovanie 2.
6. Politológia.
7. Trestné právo hmotné.
8. Trestné právo hmotné 2.
9. Operatívno-pátracia a spravodajská činnosť.
10. Moderné metódy spracovania informácií.
11. Datamining v kontexte hybridných hrozieb.
12. Kriminalistické skúmanie a vybrané druhy expetíz.
13. Kriminalistika 1.
14. Úvod do kriminalistiky .
15. Správne právo.



Príklad: Tematického plánu predmetu „Informačná bezpečnosť“

- úvod do informačnej bezpečnosti - pojem informačnej bezpečnosti, legislatívne normy z oblasti informačnej bezpečnosti a štandardy platné v oblasti informačnej bezpečnosti,
- bezpečnostná politika - cvičenie - bezpečnostná politika a zásady jej výstavby v organizácii, základné procesy bezpečnostnej politiky a základné dokumenty informačnej bezpečnosti,
- organizácia bezpečnosti - infraštruktúra informačnej bezpečnosti v organizácii, bezpečnosť prístupu tretích strán a riadenie bezpečnosti pri outsourcingu,
- klasifikácia a riadenie aktív – cvičenie - inventarizácia a klasifikácia aktív, klasifikácia údajov a informácií, klasifikácia priestorov a klasifikácia komunikačných segmentov,
- personálna bezpečnosť - bezpečnosť v definovaní práce a získavaní zamestnancov, výchovno-vzdelávací proces používateľov a zvyšovanie ich bezpečnostného povedomia, reagovanie na bezpečnostné incidenty a nefunkčnosti,
- fyzická bezpečnosť a bezpečnosť prostredia – cvičenie - režimová bezpečnosť a chránené priestory, bezpečnosť a ochrana zariadení, interné smernice a všeobecné opatrenia,
- správa počítačov a sietí - prevádzkové procedúry, plánovanie kapacít zdrojov systému a akceptácia systému, ochrana pred škodlivým softvérom, zálohovanie a archivácia informácií.

Aktivity - prevencia pred hybridnými hrozbami v rizikových skupinách

- **Identifikácia a hodnotenie rizík:** Vykonať dôkladnú analýzu hrozieb a rizík, tak aby ste identifikovali potenciálne slabé miesta a zraniteľnosti vo vašom kybernetickom prostredí.
- **Kybernetické školenia a osveta:** Poskytnúť pravidelné školenia pre svojich zamestnancov, aby boli informovaní o aktuálnych hrozbách, metódach kybernetických útokov a správnom postupe v prípade podozrivých činností.
- **Silné autentifikácie:** Zavádzať silné autentifikačné metódy, ako sú viacúrovňové overenia a dvojfaktorová autentifikácia, ktorá môže znížiť riziko neoprávneného prístupu k citlivým údajom.
- **Monitorovanie a detekcia:** Inštalovať nástroje na monitorovanie siete a detekciu podozrivých aktivít, ktoré by mohli naznačovať kybernetický útok alebo dezinformačnú kampaň.
- **Zálohovanie a obnovenie dát:** Pravidelne zálohovať dáta a vytvárať plány obnovy je veľmi dôležité, aby ste mohli rýchlo obnoviť údaje v prípade kybernetického útoku alebo sabotáže.
- **Vytváranie a uplatňovanie politík kybernetickej bezpečnosti:** Definovať jasné politiky kybernetickej bezpečnosti a zabezpečiť aby boli uplatňované vo všetkých častiach organizácie.
- **Spolupráca a informačná výmena:** Spolupracovať s inými organizáciami a vládnyimi agentúrami na zdieľaní informácií o hrozbách a najlepších postupoch v kybernetickej bezpečnosti.
- **Penetračné testy:** Pravidelne vykonávať penetračné testy, aby sa identifikovali potenciálne zraniteľnosti vo vašom kybernetickom systéme a prostredí.
- **Stály monitoring a aktualizácie:** Kybernetická bezpečnosť nie je jednorázová záležitosť. Je dôležité pravidelne monitorovať a aktualizovať bezpečnostné opatrenia, aby ste sa mohli prispôsobovať novým hrozbám a technológiám.

Aké máme problémy ?

- **Rozmanitosť útokov:** Hybridné hrozby využívajú rôznorodú škálu kybernetických útokov, ako sú phishing, ransomware, DDoS útoky, útoky na infraštruktúru a šírenie dezinformácií. Zahrnutie týchto rôznych taktík zvyšuje ich účinnosť a obmedzuje predvídateľnosť.
- **Spojenie kybernetických a fyzických útokov:** Útočníci môžu využiť slabé miesta v kybernetických systémoch na zasahovanie do fyzických zariadení alebo infraštruktúry. To môže mať vážne dôsledky pre kritické sektory, ako sú energetika, doprava alebo zdravotníctvo.
- **Ransomware kombinovaný s útokmi na dáta:** Útočníci môžu využiť ransomware na šifrovanie dôležitých dát a následne vyhroziť ich zverejnením, aby prinútili obeť platiť výkupné. Týmto spôsobom kombinujú finančnú škodu s reputačnými problémami.
- **Zneužitie internetu vecí (IoT):** Kybernetickí útočníci môžu využiť nedostatočne zabezpečené zariadenia IoT na infiltráciu do sietí, čo vedie k masívnemu zneužitiu týchto zariadení na dosiahnutie svojich cieľov, ako sú DDoS útoky (Distributed Denial of Service).
- **Hybridné špiónážne operácie:** Útočníci môžu kombinovať kybernetické útoky s tradičnými špiónážnymi technikami, aby získali citlivé informácie alebo ovplyvnili strategické rozhodnutia.
- **Zneužitie sociálnych médií:** Útočníci môžu využiť platformy sociálnych médií na šírenie dezinformácií, manipuláciu s verejnou mienkou alebo na cieľové zastrašovanie alebo zastrašovanie jednotlivcov.
- **Nízke náklady na útoky:** Kybernetické útoky majú často relatívne nízke náklady v porovnaní s tradičnými vojenskými alebo fyzickými útokmi, čo umožňuje potenciálnym útočníkom vykonávať hrozby bez vysokých investícií.

Kam sa chceme dostať ?

- vytvorenie uceleného programu vzdelávania v oblasti kybernetickej bezpečnosti a hybridných hrozieb (nové akreditované predmety – Základy KB, Teória KB1, Teória KB2, Počítačová kriminalita, **Hybridné hrozby**),
- permanentný rozvoj v danej problematike, aby bolo možné reagovať na nové výzvy,
- adekvátne personálne obsadenie pre zabezpečenie kontinuity vzdelávania (interní aj externí zamestnanci),
- moderné technologické zabezpečenie,
- aplikovať najlepšie praktické skúsenosti a použiť efektívne a účinné postupy vzťahujúce sa k súčasným bezpečnostným rizikám v súvislosti s hybridnými hrozbami,
- permanentná spolupráca so zahraničnými univerzitami,
- participácia na projektoch,
- zatriženie štúdií pre študentov APZ BA

Ďakujem za pozornosť.



Operačný program
**Efektívna
verejná správa**



Európska únia
Európsky sociálny fond



Zoznam bibliografických odkazov

ANDRAŠKO J., MESARČIK M., SOKOL P. : Právo kybernetickej bezpečnosti. 1. vyd. Bratislava: UK BA, PF, 2022, 186 s. ISBN: 978-80-7160-632-1

VON SOLMS R., VAN NIEKERK J.: *From information security to cyber security*. Computers & security. 2013, 38, s. 97-102.

ANDRESS J.: *Foundations of Information Security: A Straightforward Introduction*. No Starch Press, 2019.

<https://www.globsec.org/what-we-do/publications/ako-sa-branit-proti-informacnym-operaciám-prirucka-pre-komunikátorov>

<https://www.globsec.org/what-we-do/publications/prirucka-strategickej-komunikacie-pre-verejnu-spravu>

<https://www.enisa.europa.eu/publications/foreign-information-manipulation-interference-fimi-and-cybersecurity-threat-landscape>

https://www.japcc.org/wp-content/uploads/Joint_Air_Power_Following-_Warsaw_-Summit.pdf

<https://www.enisa.europa.eu/>

<https://www.nbu.gov.sk/wp-content/uploads/PHHD/Koncepcia-boja-SR-proti-hybridnym-hrozbam.pdf>

<https://www.minv.sk/?zvysenie-odolnosti-slovenska-voci-hybridnym-hrozbam-pomocou-posilnenia-kapacit-verejnej-spravy>

<https://www.nbu.gov.sk/wp-content/uploads/2022/08/AKCNYPAN-KOORDINACIE-BOJA-PROTI-HYBRIDNYM-HROZBAM.pdf>

<https://www.minv.sk/?informacny-system-co-1>

<https://www.minv.sk/?varovanie-obyvatelstva-1>

<https://www.akademiapz.sk/sk/pracoviska/katedry/KVSaKM>

Zákon č. 95/2019 Z.z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov

<https://www.nbu.gov.sk/>

<https://www.csirt.gov.sk/>

<https://www.bezpecnostvpraxi.sk/clanok-z-titulky/riadenie-aktiv-hrozieb-a-rizik-ttbvp.htm>

<https://www.nbu.gov.sk/urad/o-urade/hybridne-hrozby-a-dezinformacie/hybridne-hrozby/index.html>

<https://www.reserves.gov.sk/wp-content/uploads/2019/10/Terminologick%C3%BD-slovn%C3%ADk-kr%C3%ADzov%C3%A9ho-riadenia.pdf>

<https://www.toolshero.com/strategy/dimefil-framework/>

<https://euractiv.sk/tag/hybridne-hrozby/>

<https://www.nbu.gov.sk/urad/o-urade/hybridne-hrozby-a-dezinformacie/domeny/index.html>

International Organization for Standardization, International Electrotechnical Commission. ISO/IEC 15408-1:2005 Information technology — <https://touchit.sk/co-je-pegasus-a-sledovali-vas-mobil-navod-ako-to-zistit/355907>

<https://www.washingtonpost.com/opinions/2023/04/26/artificial-intelligence-democracy-danielle-allen/>

<https://www.hybridcoe.fi/wp-content/uploads/2022/06/20220623-Hybrid-CoE-Paper-14-AI-based-technologies-WEB.pdf>

<https://infosecurity.sk/facebook/nova-kniha-odhaluje-skaredu-pravdu-o-skandaloch-facebooku-a-ruskom-zasahovani-do-volieb/>

https://www.sav.sk/journals/uploads/01151315SPS_1_2017_R%20Stefik.pdf

<https://dennikn.sk/745023/ruski-hakeri-podla-expertov-utocili-na-volebny-stab-emmanuela-macrona/>

<https://ct24.ceskatelevize.cz/svet/3578097-kyberneticke-utoky-nastrojem-hybridni-valky-rusti-hackeri-cili-vyrazne-na-polsko-a>

https://www.vlada.gov.sk/share/uvsr/br-sr/sprava_o_bezpecnosti_sr_2022.pdf?csrt=16893444505740516510

<https://europskehoviny.sk/2023/05/10/v-bilcik-zneužívanie-spywaru-proti-opozícii-ci-novinarom-je-proti-hodnotam-eu/>

<https://tvnoviny.sk/domace/clanok/678331-narodna-rada-razne-zakroci-la-proti-tiktoku-zakaz-sa-vztahuje-na-vsetky-zariadenia-parlamentu>

