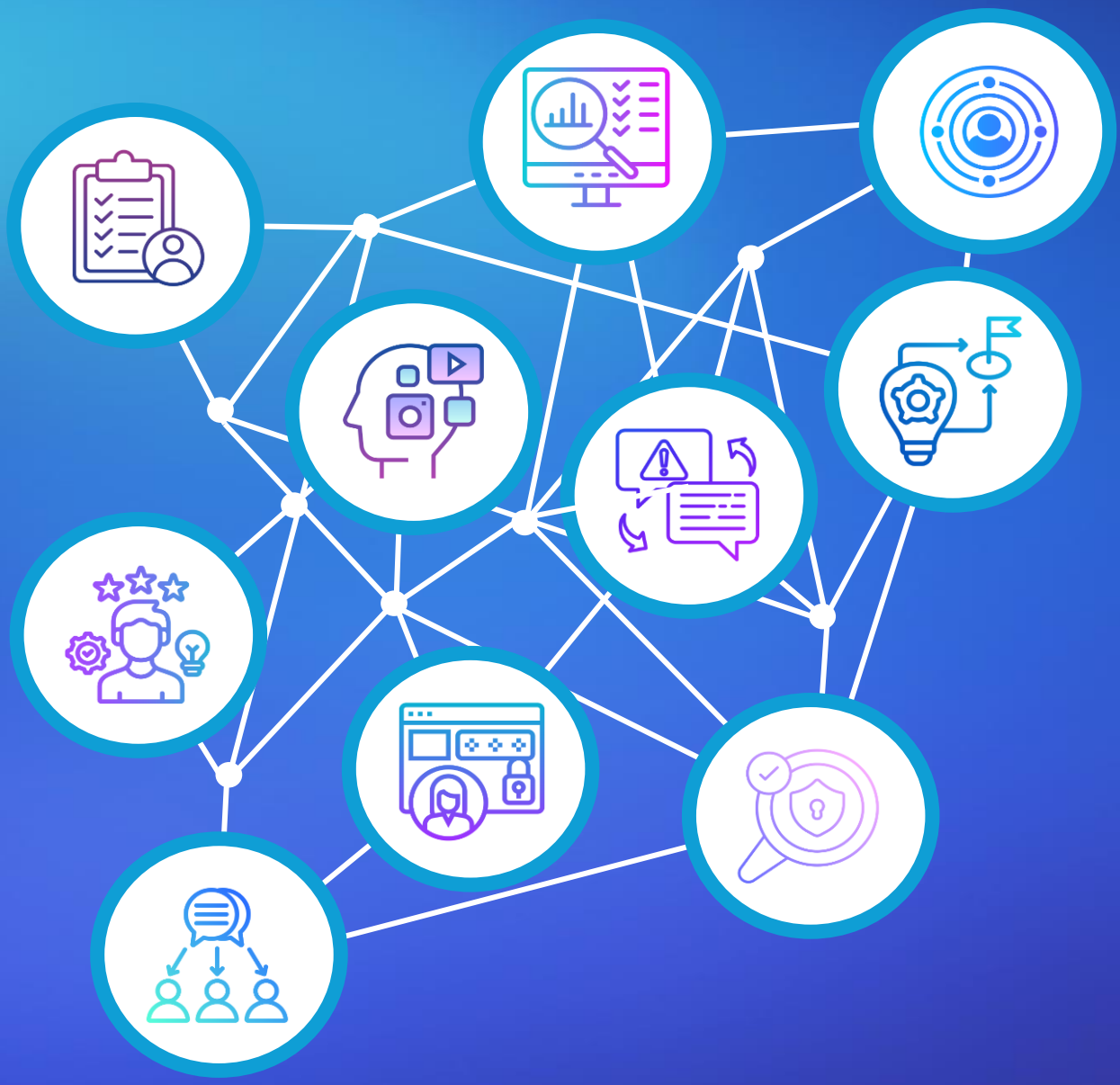


MANUÁL BEZPEČNÉHO POUŽÍVANIA SOCIÁLNYCH SIETÍ ORGÁNMI VEREJNEJ SPRÁVY

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Manuál bezpečného používania sociálnych sietí orgánmi verejnej správy

Miroslav Fečko a Ondrej Mitaľ

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Manuál bezpečného používania sociálnych sietí orgánmi verejnej správy

Autori: Miroslav Fečko a Ondrej Mitaľ

Umiestnenie: https://unibook.upjs.sk/sk/
Dostupné od: XX.11.2025

DOI: https://doi.org/

ISBN XXXX

Manuál je výstupom projektových aktivít projektu „Kompetenčné centrum kybernetickej bezpečnosti na Univerzite Pavla Jozefa Šafárika v Košiciach (KC KB UPJŠ)“ č. 17R05-04-V01-00007, ktorý je financovaný z prostriedkov mechanizmu Plánu obnovy a odolnosti .

Poďakovanie
Poďakovanie autorov patrí PhDr. Martine Pastorovej, vedúcej organizačného odboru Okresného úradu Košice, za hodnotné rady a spätnú väzbu k materiálu, čo autorom umožnilo jasne formulovať obsahové výstupy z pohľadu skúseností praxe a aplikovateľnosti zásad bezpečného používania sociálnych sietí orgánmi verejnej správy v praktickom výkone kompetencií orgánov verejnej moci.


Úvod
1
Pochopenie sociálnych sietí
Zriadenie oficiálneho účtu,
Počet oficiálnych účtov,
Odlišnosť platforiem
2
Strategický prístup
Stratégia, Politika, Dynamický vývoj
3
Odbornosť
Vzdelávanie, Tréning, Malé tímy,
Motivačné pracovné prostredie
4
Zabezpečenie stránky a účtu
Delenie zodpovednosti a pridelenie rolí, Silné heslo, Viac-faktorová autentifikácia, Neoprávnené aktivity
5
Transparentnosť a autentickosť
Kontaktné údaje, Prepojenosť účtov,
Vizuálna autentickosť,
Pravidelná aktualizácia
6
Zodpovednosť za obsah
Relevantnosť, Frekvencia zdieľania,
Zrozumiteľnosť a jasnosť,
Profesionálny obsah, Apolitický,
nestranný a objektívny
7
Orientácia na občana
Informačná kapacita, Dôvera,
Zvyšovanie participácie, angažovanosti
a zapojenia, Princíp rovnosti
8
Moderovanie diskusie
Reakcie na zdieľaný obsah,
Citlivý obsah, Názorová rôznorodosť
9
Boj s dezinformáciami
Verifikácia, Charakter reakcie,
Včasnosť reakcie
10
Monitoring
Analytika, Špecifiká používanej platformy, Riadenie rizík
Zhrnutie

Informácie o projekte

Kompetenčné centrum kybernetickej bezpečnosti na Univerzite Pavla Jozefa Šafárika v Košiciach (KC KB UPJŠ) predstavuje kompetenčné centrum, v rámci ktorého sú realizované aktivity zamerané na vzdelávanie, výskum a expertnú činnosť v oblasti informačnej a kybernetickej bezpečnosti, ochrany dát, kyberkriminality a ochrany pred dezinformáciami. Súčasne KC KB UPJŠ realizuje medzinárodnú spoluprácu s akademickými partnermi zo zahraničia a poskytuje konzultácie pre možnosť prípravy a podania projektov v oblasti kybernetickej bezpečnosti.

Vytvorenie KC KB UPJŠ reflektuje viacero problémov, ktoré možno v súčasnosti identifikovať v oblasti informačnej a kybernetickej bezpečnosti (ďalej aj „KIB“):

- zvýšenie bezpečnostného povedomia relevantných subjektov zahŕňajúcich predovšetkým zamestnancov verejnej správy a študentov vysokoškolského a stredoškolského štúdia,
- vzdelávanie a výchova nových odborníkov pôsobiacich v tejto oblasti,
- výskum kybernetických hrozieb a identifikácia adekvátnych reakcií na tieto hrozby,
- zvýšenie operatívnej bezpečnosti v rámci verejnej správy poskytovaním expertných činností zo strany CSIRT tímu.

V rámci KC KB UPJŠ sa pripravoval študijný plán magisterského stupňa študijného programu aplikovaná informatika, ktorého jedna vetva sa zameriava na kybernetickú bezpečnosť. K tomuto študijnému plánu budú vytvorené, resp. modifikované viaceré predmety. Súčasne sa ako výstup kompetenčného centrá vytvára ponuka **vzdelávania** pre rôzne cieľové skupiny zamestnancov verejnej správy.

V kontexte projektu sa súčasne posilňuje **spolupráca so strednými školami**, najmä vo forme činnosti **KyberTímov**, ich vzdelávania a následného zapojenia do šírenia bezpečnostného povedomia medzi širokou verejnosťou.

V rámci vzdelávacích aktivít sa sumarizujú nové poznatky a skúsenosti z oblasti KIB, ale aj príbuzných oblastí. Tie sú aktuálne doplnené o rôzne formy zážitkového vzdelávania.

V rámci **výskumnej** činnosti dochádza v už existujúcich výskumných oblastiach k publikovaniu viacerých vedeckých výstupov a k vytvoreniu nových možných výskumných spoluprác na posilnenie výskumného a vývojového potenciálu KC KB UPJŠ.

Nemenej dôležitým výstupom projektu je doplnenie výbavy a vzdelávanie univerzitného CSIRT tímu a možnosť poskytovania **expertných činností** pre akreditované CSIRT tímy v SR za účelom rýchlejšej a adekvátnejšej reakcie na kybernetické bezpečnostné incidenty.

Úvod

Digitálna transformácia spoločnosti ovplyvňuje súčasnú spoločnosť v rôznych oblastiach, pričom okrem iného prakticky mení spôsob, akým hľadáme, získavame, interpretujeme a šírime informácie. Výrazným spôsobom je tento proces ovplyvnený novými formami médií, medzi ktoré patria aj sociálne siete. Význam sociálnych sietí postupne narastá, a to nie len z hľadiska bežných medziľudských interakcií, plnenia cieľov podnikateľského sektora, ale aj z pohľadu plnenia úloh orgánov verejnej správy.

Nárast významu oficiálnych účtov na sociálnych sieťach využívaných na komunikáciu s verejnosťou je praktickým výsledkom digitálnej transformácie spoločnosti v oblasti komunikácie medzi orgánmi verejnej správy a verejnosťou. Sociálne médiá sú v posledných rokoch v rámci priestoru Európskej únie vnímané po televízii, ako druhý najdôležitejší informačný kanál slúžiaci na vyhľadávanie informácií o sociálnych a politických záležitostiach.[1] Na tento trend reagujú orgány verejnej správy na rôznych úrovniach spravovania spoločnosti, a to tak na celoštátnej úrovni, regionálnej úrovni, na lokálnej úrovni, ale aj na úrovni samotných politikov.

Využívanie sociálnych sietí na komunikáciu verejnej správy s verejnosťou prináša viacero benefitov, ako napríklad možnosť relatívne rýchleho šírenia informácií prakticky neobmedzenému množstvu sledujúcich, zdieľanie informácií s relatívne nízkymi nákladmi, ale aj budovanie komunity, respektíve podpora angažovanosti a zvyšovanie povedomia verejnosti. Súčasne je však potrebné vnímať, že využívanie sociálnych sietí so sebou prináša rovnako aj výzvy, a to najmä potrebu zabezpečenia autenticity informácií, boj s informačným presýtením, ale aj aktivity smerujúce k zníženiu dopadov rôznych typov škodlivého alebo nepravdivého obsahu. Aktuálne sú v krátkodobom horizonte vnímané misinformácie a dezinformácie šírené cez sociálne siete ako najväčší problém v rámci populácie respondentov mladšej ako 30 rokov a populácie medzi 30-39 rokmi života, a ako druhý najväčší problém medzi ďalšími generáciami (Svetové ekonomické fórum, 2026).[2] Bezpečná komunikácia orgánov verejnej správy v rámci sociálnych sietí sa preto javí ako dôležitý krok, vďaka ktorému je možné prispieť k šíreniu informácií so skutočnou výpovednou hodnotou pre verejnosť.

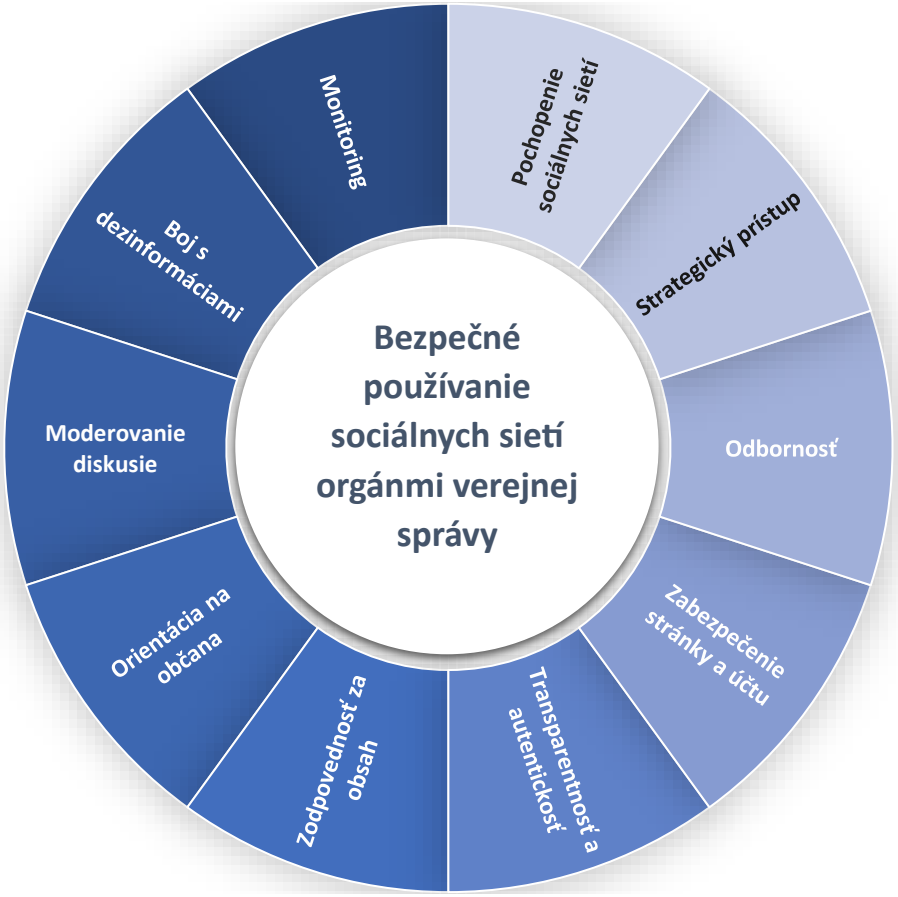
Vychádzajúc z potreby využívať sociálne siete ako jeden z informačných kanálov orgánmi verejnej správy, a uvedomujúc si riziká a výzvy týchto digitálnych platforiem, je potrebné formulovať hlavné a východiskové zásady a princípy bezpečného používania sociálnych sietí orgánmi verejnej správy. Zásady a princípy bezpečného používania sociálnych sietí v podobe manuálu predstavujú súbor odporúčaní, ktoré sú v súčasných kontextoch najvýznamnejšie pre bezpečnú komunikáciu orgánov verejnej správy na sociálnych sieťach.

[1] Európsky parlament (2025). Social Media Survey 2025. [cit 4/3/2026]. Dostupné online: https://europa.eu/eurobarometer/api/deliverable/download/file?deliverableId=100969

[2] Svetové ekonomické fórum (2026). Global Risks Report 2026. [cit 4/3/2026]. Dostupné online: https://reports.weforum.org/docs/WEF_Global_Risks_Report_2026.pdf

Desať zásad a princípov je možné považovať za súbor odporúčaní, ktoré sa v dnešnej dobe ukazujú ako najdôležitejšie.

Každá z desiatich hlavných zásad je dekomponovaná prostredníctvom čiastkových bodov.



Tempo technologického pokroku a spoločenských zmien vyplývajúcich z digitálnej transformácie spoločnosti predpokladá, že súbor identifikovaných princípov a zásad nie je nemenný, ale časom musí podliehať zmenám, ktoré budú odzrkadľovať urgentnosť a reflektovať aktuálne skúsenosti

POCHOPENIE SOCIÁLNYCH SIETÍ

Zriadenie oficiálneho účtu

Počet oficiálnych účtov

Odlišnosť platforiem

1 Pochopenie sociálnych sietí

Rozhodnutie orgánu verejnej správy vytvoriť oficiálnu stránku na sociálnej sieti je v súčasnosti racionálnym dopadom digitálnej transformácie spoločnosti. Predpokladom bezpečného využívania sociálnych sietí je **pochopenie platforiem**, a to predovšetkým cez kľúčové funkcionality, ktoré orgánom verejnej správy jednotlivé platformy ponúkajú.

Zriadenie oficiálneho účtu orgánu verejnej správy na sociálnych sieťach by nemalo byť vnímané ako náhodný sled udalostí, ale práve naopak, ako výsledok snahy orgánu verejnej správy byť bližšie k verejnosti. Využitie sociálnych sietí vo verejnej správe je možné v súčasnosti vnímať ako trend, vďaka ktorému je možné k verejnosti dostať správne, včasné a autentické informácie aj inak, ako prostredníctvom tradičných komunikačných kanálov.

Orgán verejnej správy preto má možnosť rozhodnúť sa, aký **počet oficiálnych účtov** na sociálnych sieťach bude využívať. Toto rozhodnutie je dané viacerými faktormi a môže sa výrazne odlišovať prístupom konkrétneho subjektu verejnej správy k tomuto trendu. V prvom rade ide o charakter riadenia orgánu verejnej správy, ktorý v tomto kontexte reflektuje počet zamestnancov, informačnú stratégiu, marketingovú stratégiu, ale aj dostupnosťou využiteľných finančných zdrojov. Súčasne však je potrebné brať do úvahy aj charakter oslovovaného publika, ktorý je daný najmä jeho počtom, demografickými vlastnosťami obyvateľov, ale aj zámerom osloviť špecifických aktérov verejnej politiky (firmy, univerzity, občianske iniciatívy a iné).

Orgán verejnej správy by mal dbať na to, aby na jednej a tej istej platforme sociálnych sietí zriadil len jeden oficiálny účet. Nie je potrebné, aby viaceré oddelenia a odbory jedného orgánu verejnej správy mali svoje vlastné účty na sociálnych sieťach. Oficiálny účet orgánu verejnej správy má slúžiť ako nástroj jednotnej komunikácie a ako zdroj relevantných a overených informácií v celej kompetenčnej šírke daného orgánu verejnej správy.

Počet platforiem sociálnych sietí sa neustále zvyšuje, pričom tento nárast reflektuje **odlišnosť platforiem**. Orgány verejnej správy by preto pri výbere vhodnej platformy mali zohľadniť viacero hľadísk, a to najmä s ohľadom na predispozície používateľov využívajúcich konkrétnu platformu, charakter a formu zdieľaného obsahu, ale aj popularitu, etablovanosť a potenciál konkrétnej platformy.

Zodpovedaním uvedených otázok je možné dospieť z pohľadu orgánu verejnej správy k pochopeniu úlohy sociálnych sietí pre verejnú správu a občanov. Zároveň je následne možné stanoviť jasný koncept, ktorý by mal byť transformovaný do konkrétnej politiky alebo stratégie. V opačnom prípade je prezencia orgánu verejnej správy na sociálnych sieťach len nesofistikovanou a nepredvídateľnou aktivitou bez schopnosti naplniť očakávania verejnosti.

STRATEGICKÝ PRÍSTUP

Stratégia

Politika

Dynamický vývoj

2 Strategický prístup

Strategický prístup je nevyhnutný pri komplexnosti a sofistikovanosti funkcionalít platforiem sociálnych sietí z pohľadu orgánov verejnej správy. V praktickom slova zmysle je takáto ambícia transformovaná spravidla do podoby stratégie alebo politiky. Práve vďaka jasnému stanoveniu predvídateľných pravidiel a postupov je možné dosiahnuť bezpečnejšie používanie sociálnych sietí, pretože vďaka nim je možné reagovať na prípadne výzvy a incidenty.

Stratégia orgánov verejnej správy zameraná na využívanie sociálnych sietí by vo všeobecnosti mala byť zameraná na vyhodnotenie aktuálneho stavu, analýzu trendov pri využívaní orgánmi verejnej správy, a v konečnom dôsledku stanovenie cieľov, ktoré by mali byť relevantné, dosiahnuteľné a monitorovateľné. Súčasne je možné stratégiou stanoviť aj špecifické náležitosti, ako napríklad design manuál, formálne a obsahové náležitosti zdieľaných informácií, a iné.

Formulovaná stratégia okrem iného obsahuje aj jasné vymedzenie cieľovej skupiny, ktorá má byť oslovená informačným obsahom na konkrétnych sociálnych sieťach. Orgány verejnej správy by teda mali vedieť jasne vymedziť, aké publikum chcú informáciou osloviť a na ktorej platforme sociálnych sietí dané publikum nájdu.

Paralelne s existenciou stratégie, **politika** sociálnych médií vo verejnej správe by mala koncentrovať pozornosť na kľúčové náležitosti využívania jednotlivých platforiem, a to najmä manažment účtov a rolí, bezpečnostné otázky, úpravu interakcií na oficiálnych účtoch zo strany zamestnancov a občanov, charakter a formu zdieľaného obsahu, a ďalšie.

Opodstatnenosť strategického prístupu pri využívaní sociálnych sietí orgánmi verejnej správy je navyše ovplyvňuje aj **dynamický vývoj** samotných platforiem. Na jednej strane by stratégie a politiky mali symbolizovať nástroj koncepčného a cieleného využívania sociálnych sietí v súlade s potrebami orgánov verejnej správy. Na druhej strane je žiadúca krátkodobá periodicita doplnenia a aktualizácie, pretože k zmenám existujúcich funkcionalít a rozširovaniu nových funkcionalít nedochádza v horizonte rokov, ale mesiacov.

ODBORNOSŤ

Vzdelávanie

Tréning

Malé tímy

Motivačné pracovné prostredie

3 Odbornosť

Dôležitým prvkom spravovania oficiálnych účtov je **odbornosť** zodpovedných osôb, pretože práve od ich vedomostí a znalostí záleží kvalita zdieľaného obsahu a informácií, ktoré sú dostupné širokej verejnosti. Spravovanie oficiálnych účtov na sociálnych sieťach by malo byť realizované zamestnancami, ktorí sa na túto činnosť dlhodobo špecializujú. Špecializácia je v tomto ohľade kľúčová bez ohľadu na to, či sú zamestnanci takto dlhodobo profilovaní v samotných orgánoch verejnej správy, alebo sú podľa potreby doplnení do tímu, respektíve oddelenia z externého prostredia.

Zamestnanci podieľajúci sa na spravovaní oficiálnych účtov na sociálnych sieťach musia byť v tejto problematike dlhodobo a systematicky vzdelávaní a trénovaní. **Vzdelávanie** umožní zamestnancom získať informácie o zmenách a vylepšeniach v kľúčových aspektoch používania sociálnych sietí, ako aj aktuálnych trendoch. Zároveň však rozvíja znalosti nevyhnutné pre pokročilé využívanie v podobe zacielenia vhodného publika, pokročilej analytiky, využívaní reklamy a tvorby obsahu.

Tréning na druhej strane umožňuje zamestnancom získať schopnosti, vďaka ktorým bude zlepšená ich kompetentnosť reagovať na prípadné riziká a problémy, ktoré pri spravovaní oficiálnych účtov na sociálnych sieťach môžu nastať. Zameranie tréningov pre oblasť správy oficiálnych účtov na sociálnych sieťach je preto najčastejšie zamerané na bezpečnosť používania účtov, boj s dezinformáciami, moderovanie komunikácie s občanmi a iné.

Úspešnosť dosahovania cieľov v orgánoch verejnej správy je spravidla zabezpečená správou oficiálnych účtov **v malých tímoch**, v rámci ktorých existujú jasné zodpovednosti, ale zároveň je spoľahlivo navrhnutá zastupiteľnosť v rámci zodpovednosti jednotlivých členov tímu. Tím spravujúci sociálne siete zároveň nemá pôsobiť ako autonómna a samo-rozhodujúca jednotka. Schválenie plánu a obsahu príspevkov zo strany vedenia orgánu verejnej správy prispieva k napĺňaniu nadradeného cieľa, ktorým je prezentácia relevantných a faktických informácií pre verejnosť.

Vhodné a **motivačné pracovné prostredie** bezprostredne súvisí so zodpovednosťou za spravovanie účtu, ktorého obsah je dostupný širokej verejnosti a nie len vybraným osobám ako je to v prípade súkromných profilov. Nevyhnutnosťou je taktiež kvalitné a zodpovedajúce technické vybavenie tímu, ktoré spočíva najmä v adekvátnom vybavení počítačmi, smartfónmi, prípadne video a zvukovou technikou. Súčasne je však dôležité, aby bol zodpovedný tím alebo zodpovední jednotlivci súčasťou organizačnej štruktúry a boli pozitívne vnímaní a rešpektovaní zo strany ďalších zamestnancov, ktorých výsledky a výstupy práce prezentujú širšiemu publiku.

Odborne zdatný zamestnanec spravujúci oficiálne účty orgánov verejnej správy na sociálnych sieťach je práve vďaka vzdelávaniu, tréningu a vhodnému pracovnému prostrediu dôležitým elementom bezpečného využívania sociálnych sietí vo verejnej správe.

ZABEZPEČENIE STRÁNKY A ÚČTU

Delenie zodpovedností a pridelenie rolí

Silné heslo

Viac-faktorová autentifikácia

Neoprávnené aktivity

4 Zabezpečenie stránky a účtu

Bezpečné používanie sociálnych sietí zo strany orgánov verejnej správy predpokladá aj kvalitné a systematické **zabezpečenie stránky a účtu**, prostredníctvom ktorého orgány verejnej správy komunikujú s verejnosťou. Zabezpečenie do veľkej miery závisí od bezpečnostných funkcionalít samotnej platformy sociálnej siete. Z hľadiska ľudského faktora zabezpečujúceho správu oficiálnej stránky alebo účtu, je však nevyhnutné túto bezpečnosť doplnkovo posilniť jasným stanovením pravidiel.

Bezpečnosť oficiálnych účtov orgánov verenej správy na sociálnych sieťach je v prvom rade zabezpečená najmä cez **delenie zodpovedností a pridelenie rolí** v rámci spravovania oficiálnych účtov. Možnosti prideľovanie hierarchických rolí pre zamestnancov spravujúcich oficiálne účty sú samozrejme špecificky dané charakterom konkrétnej platformy. V záujme zachovania čo najvyššej možnej miery bezpečnosti je však potrebné prideliť plnú kontrolu nad oficiálnym účtom orgánu verejnej správy na sociálnych sieťach čo najmenšiemu okruhu zamestnancov. Počet zamestnancov zodpovedných za spravovanie samotného obsahu následne môže byť prirodzene širší. Počty zodpovedných zamestnancov sa môžu odlišovať, pretože v konečnom dôsledku reflektujú veľkosť tímu zabezpečujúceho správu sociálnych sietí v orgáne verejnej správy, ale zároveň je veľkosť tímu závislá aj od racionálneho pomeru k počtu zamestnancov konkrétneho úradu orgánu verejnej správy.

K bezpečnosti spravovania oficiálnych účtov orgánov verejnej správy na sociálnych sieťach prispieva aj **silné heslo**. Zabezpečenie prístupu k účtu silným heslom je už na jednotlivých platformách nevyhnutné pri samotnej registrácii. Možnosťou ako posilniť heslo je vytvorenie odlišných hesiel pri rôznych platformách. Poskytovanie hesla mimo okruhu osôb, ktoré spravujú oficiálne profily možno považovať za neprípustné. K ochrane hesla prispieva aj vedomosť, že samotné platformy prevádzkujúce sociálne siete nevyžadujú zadávanie hesiel mimo platformy, ako napríklad prostredníctvom e-mailu alebo sms správ. Silné heslo tak v konečnom dôsledku chránia zodpovedné osoby.

Vzhľadom na nárast aktivít smerujúcich ku krádeži identít na sociálnych sieťach je dôležitým nástrojom aj **viac-faktorová autentifikácia**, ktorá je paralelne využívaná spolu so silným heslom. Dvoj-faktorová autentifikácia je druhým krokom, vyžadujúcim ďalšiu verifikáciu prihlasujúceho sa používateľa, ktorým je správca oficiálneho účtu orgánu verejnej správy na sociálnej sieti. Najbežnejšími a osvedčenými spôsobmi potvrdzovania dvoj-faktorovej autentifikácie sú zadávanie kódu zaslaného textovou správou alebo využitie autentifikačnej aplikácie v rámci smart telefónu.

Silné heslo aj dvoj-faktorová autentifikácia výrazne prispievajú k posilneniu bezpečnosti používania sociálnych sietí orgánmi verejnej správy. Napriek tomu však nie je možné zabrániť prípadným pokusom o neúspešné prihlásenie sa do účtov na konkrétnych platformách. Z pohľadu orgánov verejnej správy je preto žiadúce **sledovať, vyhodnocovať a nahlasovať neoprávnené aktivity** v súlade s postupom stanoveným konkrétnou platformou. Taktiež je dôležité reagovať na duplicitné a podvodné aktivity, ktoré sa snažia vystupovať v mene orgánov verejnej správy prostredníctvom falošných stránok a účtov.

TRANSPARENTNOSŤ A AUTENTICKOSŤ

Kontaktné údaje

Prepojenosť účtov

Vizuálna autentickosť

Pravidelná aktualizácia

5 Transparentnosť a autentickosť

Oficiálny účet orgánu verejnej správy na sociálnych sieťach by mal sledovať **najvyššie štandardy transparentnosti a autentickosti**. Široká verejnosť by nemala mať pochybnosť o tom, že predmetný účet na sociálnej sieti je skutočne oficiálnou stránkou konkrétneho orgánu verejnej správy. Prioritným zámerom orgánu verejnej správy by malo byť dosiahnutie stavu, kedy sú vyplnené a zverejnené všetky dôležité informácie o oficiálnej stránke v závislosti od možností konkrétnej platformy.

Autentickosť oficiálneho účtu je možné jednoducho verifikovať v prípade, že účet má plne vyplnené všetky základné informácie. K týmto informáciám vieme zaradiť **kontaktné údaje**, ktorých obsah sa môže v závislosti od konkrétnej platformy odlišovať, avšak ide najmä o adresu, telefonický kontakt a e-mailová adresa. Tieto kontaktné údaje ponúkajú verejnosti priestor na veľmi jednoduchú verifikáciu. Doplnkovo je možné zverejniť aj ďalšie všeobecné informácie, ako napríklad rozpis úradných hodín.

Pri oficiálnych účtoch orgánov verejnej správy na sociálnych sieťach je taktiež žiadúca aj vzájomná **prepojenosť účtov** na rôznych platformách. Povedané inak, je nevyhnutné, aby na seba jednotlivé komunikačné a informačné kanály orgánov verejnej správy priamo odkazovali. Konkrétne je dôležité, aby oficiálne účty na sociálnych sieťach priamo odkazovali na oficiálnu webovú stránku orgánu verejnej správy, a naopak. Zároveň je v súčasnosti možné, aby aj samotné oficiálne účty na jednej sociálnej sieti obsahovali informáciu o existencii oficiálnych účtov na iných sociálnych sieťach. Prepojenosť účtov v tomto ohľade súvisí aj s prepojením obsahu, ktorý je prezentovaný zo strany orgánu verejnej správy. V rovnakom čase by prezentované informácie na rozličných platformách mali mať rovnakú obsahovú náplň.

Popri základných informáciách je dôležitá aj **vizuálna autentickosť**, ktorú je možné najčastejšie vnímať cez oficiálne logo orgánu verejnej správy, prípadne erb a logo v prípade orgánov územnej samosprávy. V ideálnom prípade by grafický design používaných grafík mal kopírovať oficiálne alebo zaužívané farby, ktorými sa orgán verejnej správy bežne prezentuje.

K transparentnosti a autentickosti pomáha aj to, aby bola zabezpečená **pravidelná aktualizácia** základných informácií a obsahu dostupného na oficiálnej stránke. V opačnom prípade tak oficiálny účet orgánu verejnej správy na sociálnych sieťach stráca vierohodnosť a prestáva byť bezpečným komunikačným kanálom medzi verejnou správou a verejnosťou. Pravidelné aktualizácie by však nemali vo výsledku viesť k zdieľaniu všetkého, čo sa v rámci orgánu verejnej správy deje.

Transparentnosť a autentickosť oficiálneho účtu na sociálnych sieťach je preto možné vnímať ako ďalší prvok, ktorým je možné posilniť bezpečnosť využívania sociálnych sietí v interakcii verejnej správy s verejnosťou. V prípade dodržania uvedených odporúčaní je možné povedať, že orgán verejnej správy urobil zásadný krok k tomu, aby oficiálna stránka alebo účet nemohli byť ľahko zameniteľné s iniciatívou poskytujúcou verejnosti zavádzajúci a škodlivý obsah.

ZODPOVEDNOSŤ ZA OBSAH

Relevantnosť

Frekvencia zdieľania

Zrozumiteľnosť a jasnosť

Profesionálny obsah

Apolitický, nestranný a objektívny

6 Zodpovednosť za obsah

Orgány verejnej správy nesú **zodpovednosť za zdieľaný obsah** na sociálnych sieťach, pričom ich primárnym cieľom má byť sledovanie a podporovanie verejného záujmu. Tento obsah by mal byť tvorený tak, aby podporoval bezpečnú komunikáciu orgánu verejnej správy a verejnosti.

Zdieľaný obsah a jeho **relevantnosť** je prvým aspektom rozhodujúcim o kvalite informácie. Relevantnosť zdieľaných informácií a obsahu sa v konečnom dôsledku odvíja od stratégie a politiky konkrétneho orgánu verejnej správy, a to najmä vo vzťahu k charakteru zdieľanej informácie a publiku, ktorému je určená. Vo všeobecnosti platí, že každý zdieľaný obsah by mal mať pre ostatných používateľov pridanú hodnotu. V opačnom prípade môže dôjsť k presýteniu občana nerelevantným obsahom, a verejná správa potom nepodporuje bezpečnú komunikáciu na sociálnych sieťach, ale práve naopak, podporuje zahltenie a presýtenie informačného prostredia.

Relevantnosť zdieľaného obsahu súvisí tiež s ďalším aspektom, ktorým je **frekvencia zdieľania**. Nadmerná frekvencia zdieľania na oficiálnych účtoch môže rovnako smerovať k informačnému presýteniu občana, a teda nemožnosti rozpoznať, ktorá informácia je alebo nie je dôležitá. Zahltenie málo relevantným obsahom by viedlo k opačnému efektu a k degradácii účelu spravovaného účtu.

Súčasne je nevyhnutná aj **zrozumiteľnosť a jasnosť** zdieľaného obsahu. Sociálne siete svojím charakterom smerujú k tomu, že zdieľaný obsah má byť skôr stručný a krátky, a teda sociálne siete nie sú určené na zdieľanie nadmerne objemného množstva textu a dát. Priestor, ktorý je orgánom verejnej správy ponúkaný prostredníctvom postov, fotografií, respektíve video obsahu by mal byť využitý tak, aby verejnosť vedela efektívne zdieľaný obsah spracovať, využiť vo svoj prospech, prípadne zdieľať.

Orgány verejnej správy by mali na svojich oficiálnych účtoch zverejňovať **profesionálny obsah**. Zdieľaný obsah by mal byť kvalitatívne na vyššej úrovni, ako bežný obsah zdieľaný súkromnými účtami, keďže je určený pre širokú verejnosť. Z formálneho hľadiska by obsah mal byť zdieľaný s využitím sofistikovanej grafiky, ktorá dotvára celkový image konkrétneho orgánu verejnej správy. Ak už aj nie je obsah pripravený na základe odbornosti zamestnancov zodpovedných za správu oficiálnych stránok, mal by byť zodpovednými osobami upravený do podoby spĺňajúcej aspoň minimálne štandardy kvality.

Informácie by mali byť zdieľané spôsobom, aby obsah bol **apolitický, nestranný a objektívny**. Apolitickosť je nevyhnutným kvalitatívnym aspektom zdieľaných informácii, a to najmä preto, že politický aspekt riadenia orgánov verejnej správy je neoddeliteľnou súčasťou demokratických procesov. Oficiálne účty by preto nemali byť využívané ako nástroj počas politickej kampane. Nestrannosť zdieľaného obsahu je dôležitá najmä preto, že z pohľadu orgánu verejnej správy je potrebné eliminovať vplyv tretích strán, ktoré by mohli mať záujem ovplyvniť správanie, konanie alebo rozhodovanie verejnosti práve prostredníctvom oficiálneho účtu. Zdieľaný obsah je objektívny vtedy, ak je očistený od akéhokoľvek subjektívneho presvedčenia osôb zodpovedných za správu oficiálneho účtu, ale aj vedenia orgánu verejnej správy. Vypracovanie internej smernice, ktorá by okrem iného upravila aj prípadné porušenie zodpovednosti za zdieľaný obsah by prispela k vnútorným pravidlám, ktoré sú pre zamestnancov orgánu verejnej správy predvídateľné a v prípade potreby aj vynútiteľné.

ORIENTÁCIA NA OBČANA

Informačná kapacita

Dôvera

Zvyšovanie participácie, angažovanosti a zapojenia

Princíp rovnosti

7 Orientácia na občana

Informačná kapacita verejnosti je komplexný súbor dlhodobých procesov, ktorý vie byť v kontexte celkovej informačnej stratégie orgánov verejnej správy podporený aj spôsobom, akým verejnosť získava, chápe a zdieľa informácie zverejňované na sociálnych sieťach. Sociálne siete a oficiálne stránky orgánov verejnej správy preto musia byť využívané takým spôsobom, kedy je zvyšovaná **informačná kapacita** verejnosti.

Adekvátnym využívaním oficiálnych účtov na sociálnych sieťach môže byť pozitívne ovplyvnená aj **dôvera** v orgány verejnej správy. Dôvera v tomto zmysle býva vnímaná ako tendencia verejnosti dôverovať v správnosť výkonu kompetencií a realizácie verejných politík. Oficiálne účty na sociálnych sieťach podporujú dôveru v orgány verejnej správy prioritne vďaka šíreniu pozitívnych informácií o zrealizovaných projektoch, organizovaných podujatiach, respektíve dosiahnutých úspechoch pri riešení podnetov verejnosti a rozvoji územia.

Oficiálne účty orgánov verejnej správy na sociálnych sieťach by mali slúžiť okrem iného aj ako nástroj, prostredníctvom ktorého je možné systematické **zvyšovanie participácie, angažovanosti a zapojenia obyvateľov**. Systematickým a cieleným informovaním prostredníctvom bezpečnej komunikácie je možné vo verejnosti vytvoriť stav, kedy budú sociálne siete vnímané ako informačný kanál, na základe ktorého je možné pozitívne ovplyvniť verejný záujem a podporiť spoluprácu s verejnosťou pri tvorbe a implementácii verejných politík. K uvedenému prispieva aj zachovanie kontinuity a zavedeného prístupu k využívaniu účtov na sociálnych sieťach, a to aj v prípade zmien vo vedení konkrétnych orgánov verejnej správy.

Obsahom zdieľaným na oficiálnych účtoch orgánov verejnej správy na sociálnych sieťach by malo byť oslovené čo najširšie publikum v celej jeho rôznorodosti, čím je podporený **princíp rovnosti**. V tomto zmysle by mali byť oficiálne stránky na sociálnych sieťach využívané tak, aby bol ich obsah využiteľný všetkými obyvateľmi bez ohľadu na ich demografické charakteristiky a úroveň dosiahnutej gramotnosti využívania sociálnych sietí.

MODEROVANIE DISKUSIE

Reakcie na zdieľaný obsah

Citlivý obsah

Názorová rôznorodosť

8 Moderovanie diskusie

Sociálne siete ponúkajú orgánom verejnej správy priestor na obojsmernú bezprostrednú online komunikáciu s verejnosťou, v rámci ktorej vzniká žiadúca, autentická, ale zároveň aj veľmi ťažko predvídateľná diskusia. Z pohľadu verejnej správy je kľúčové **moderovanie diskusie**, ktorá je podnietená zdieľaným obsahom, a to v kontexte vytvorenia bezpečného informačného prostredia pre verejnosť.

Oficiálny účet orgánu verejnej správy síce prezentuje obsah vygenerovaný osobami zodpovednými za správu účtu, avšak **reakcie na zdieľaný obsah** môžu nadobúdať rôzny charakter. Samotná verejnosť v postavení bežných používateľov sociálnych sietí môže reagovať na zdieľaný obsah v pozitívnom, negatívnom, ale aj rozporuplnom zmysle. Úlohou verejnej správy je preto zabezpečiť, aby prípadnými negatívnymi alebo rozporuplnými reakciami nedošlo k skresleniu, prípadne znehodnoteniu pôvodnej zdieľanej informácie. Prirodzeným výsledkom reakcií na zdieľaný obsah by mala byť konštruktívna diskusia, založená na faktoch a pozitívnom pokračovaní a rozvíjaní komunikácie.

Vysoká úroveň sofistikovanosti súčasných spoločenských interakcií zároveň pre orgány verejnej správy znamená, že musia prostredníctvom svojich oficiálnych účtov na sociálnych sieťach zdieľať a následne aj moderovať **citlivý obsah**. Pri určitých typoch informácií je možné očakávať, že reakcia verejnosti bude mať charakter emotívnej reakcie založenej na hneve, nespokojnosti, kritike alebo frustrácii. Moderovanie diskusie zamestnancov zodpovedných za správu oficiálnych účtov musí byť v týchto prípadoch racionálne a neemotívne. Verejná správa zároveň nemôže pripustiť, aby prípadné reakcie a diskusia na zdieľaný obsah smerovala k polarizácii, či šíreniu urážlivých a nepravdivých informácií.

Pokiaľ dochádza k moderovaniu diskusie a k prípadným doplneniam vo forme komentárov, je nevyhnutné, aby sa bežní zamestnanci orgánu verejnej správy priamo nezapájali do názorovej výmeny. Moderovanie a reakcie majú byť súčasťou práce tímu, ktorým má sociálne siete na starosti. Aj príliš rýchla reakcia, alebo reakcia ktorá nebola konzultovaná s vedením organizácie, môže diskusiu viac burcovať ako emócie upokojovať. Zamestnanci orgánu verejnej správy, ktorí nemajú na starosti správu účtov na sociálnych sieťach, by mali dbať na profesionálny prístup spočívajúci vo vysvetľovaní a argumentovaní občanom v rozsahu svojej zverenej oblasti a komunikačnými kanálmi na to vhodnými (osobne, emailová komunikácia, poštou, telefonicky počas úradných hodín a pod.).

Výsledkom moderovania diskusie zo strany orgánov verejnej správ by však nemala byť limitácia a popieranie názorovej rôznorodosti, ani cielené odstraňovanie prejavov názorových oponentov. **Názorová rôznorodosť** a konštruktívna diskusia je integrálnou súčasťou demokratickej spoločnosti a má svoje pevné miesto aj v prostredí sociálnych sietí.

BOJ S DEZINFORMÁCIAMI

Verifikácia

Charakter reakcie

Včasnosť reakcie

9 Boj s dezinformáciami

Sociálne siete ponúkajú verejnej správe unikátnu platformu na komunikáciu s verejnosťou, ktorá prináša veľké množstvo výhod. Súčasne sú však sociálne siete vnímané aj ako priestor, na šírenie nepravdivých a škodlivých informácií. Orgány verejnej správy preto môžu využívať svoje oficiálne účty aj na **boj s dezinformáciami**, vďaka čomu je možné prispieť k nižšej miere šírenia dezinformácií, a teda bezpečnejšej komunikácii.

Verejná správa vo svojej podstate prirodzene bojuje s dezinformáciami. Pri zdieľaní akéhokoľvek obsahu musí prebehnúť **verifikácia**, či je zdieľaný obsah pravdivý a relevantný. Na oficiálnych účtoch orgánov verejnej správy na sociálnych sieťach by totiž v žiadnom prípade nemal byť zdieľaný obsah, ktorý nadobúda parametre dezinformácie z pohľadu škodlivosti alebo nepravdivosti informácie.

Verejná správa môže využiť odlišný **charakter reakcie** vo vzťahu ku konkrétnym typom dezinformácií a ich negatívnym dopadom. Úlohou orgánov verejnej správy je prispieť k boju proti aktuálne šíreným dezinformáciám v spoločnosti, ktoré svojím vplyvom presahujú priestorový rámec komunít, miest alebo regiónov. Zároveň je ale žiadúce, reagovať z pozície orgánov verejnej správy aj v prípade lokálne konkrétnych, špecifických dezinformácií, ktoré majú priamy dopad na lokálnu komunitu. Kľúčovým aspektom pri boji s dezinformáciami je využívanie faktov, ktoré prispievajú k tomu, že pôvodná sila vplyvu dezinformácie sa postupne vytráca.

Orgány verejnej správy by v prípade reakcie na dezinformácie mali rešpektovať tematickú oblasť, ktorú v štruktúre verejnej správy majú kompetenčne na starosti. Orgán verejnej správy by sa tak mal vyjadrovať len k tým témam, ktoré sú obsahom dezinformácií, ktoré priamo spadajú do kompetencií daného orgánu. V prípade snahy podporiť vyvrátenie dezinformácie tematicky sa týkajúcej iného orgánu verejnej správy, respektíve iného rezortu, je vhodnejšia forma zdieľania vysvetľujúceho príspevku príslušného orgánu verejnej správy.

Pri boji s dezinformáciami je zároveň nevyhnutné zabezpečiť **včasnosť reakcie**, pretože nie len objektívna ale aj skorá reakcia pomáha zabrániť ďalšiemu šíreniu dezinformácie. Znižuje sa tým jej potenciálny negatívny vplyv na ďalších užívateľov sociálnych sietí. Zároveň však platí, že na podstatnú časť dezinformácií je možné reagovať až následne, teda až keď sú súčasťou informačného priestoru a negatívne toto informačné prostredie ovplyvňujú.

MONITORING

Analytika

Špecifiká používanej platformy

Riadenie rizík

10 Monitoring

Bezpečné využívanie oficiálnych účtov orgánov verejnej správy na sociálnych sieťach predpokladá aj systematické a cielené aktivity, ktorých obsahom je **monitoring** a následná analýza dát. Komplexnosť, ktorú sociálne siete ponúkajú šíriteľom obsahu, je priamo reflektovaná šírkou zhromažďovaných dát o samotnom oficiálnom účte.

Pre monitorovanie úspešnosti zdieľaného obsahu z pohľadu efektívnosti dosahovania stanovených cieľov je kľúčová **analytika**, ktorá je poskytovaná jednotlivými platformami sociálnych sietí. Analytika spravidla poskytuje informácie o úspešnosti zdieľaného obsahu, najmä šírke zasiahnutého publika, dĺžke získanej pozornosti, a samozrejme aj množstve reakcií zo strany bežných užívateľov. Analýza dát poskytovaných sociálnymi sieťami je kľúčová pre ďalšie rozhodovanie o tom, aký obsah bude zdieľaný. Rozhodnutia, ktoré orgány verejnej správy môžu na základe analýzy dát prijať, môžu byť zamerané na rôzne aspekty zdieľania obsahu, a to najmä redefinovanie a špecializácia zdieľaných informácií, zmena času zdieľania, zmena formátov a grafiky zdieľaného obsahu, ale aj zvýšenie frekvencie zverejňovania obsahu.

Sledovanie analytiky a užívateľských trendov je zároveň potrebné v čase vyhodnocovať a prispôsobovať **špecifikám používanej platformy**. Platformy sociálnych sietí postupom času môžu meniť svoj algoritmus, ktorý rozhoduje o úspešnosti zdieľaného obsahu. Prístup k zdieľaniu obsahu, ktorý sa orgánu verejnej správy po nejakú dobu osvedčil, nemusí byť stále rovnako efektívny. To čo fungovalo dnes, zajtra nemusí byť rovnako účinné. Orgány verejnej správy by preto mali vyhodnocovať, či zdieľanie obsahu na konkrétnej platforme sociálnych sietí stále plní účel a ciele, na základe ktorých sa orgán verejnej správy rozhodol vytvoriť svoj oficiálny účet, respektíve stránku.

Využívanie nových digitálnych médií so sebou prináša pre verejnú správu aj výzvy, ktoré je možné zvládnuť prostredníctvom súborov procesov, ktoré súhrnne nazývame **riadenie rizík**. Samotné riadenie rizík automaticky predvída, že konkrétne riziko môže v skutočnosti nastať, a preto orgány verejnej správy prideľujú rôznym rizikám rôznu mieru pravdepodobnosti výskytu, stanovujú spôsob ich monitorovania, ale aj možnosti ich riešenia. K najčastejším rizikám vo verejnej správe môžeme zaradiť najmä ohrozenie reputácie, zneužitie zdieľaného obsahu, neoprávnené využívanie oficiálneho účtu, politická manipulácia, ale aj zneužitie analytiky na sledovanie.

Opierajúc sa o relevantnú analytiku a v snahe podporiť šírenie a zviditeľnenie príspevkov môžu orgány verejnej správy zapojiť spolupracujúce subjekty a organizácie, a to napríklad formou pozvania na spoluprácu pri konkrétnych príspevkoch, alebo vzájomným zdieľaním vybraných príspevkov na sociálnych sieťach.

Zhrnutie

Manuál bezpečného používania sociálnych sietí orgánmi verejnej správy prezentuje zásady a princípy, ktoré predstavujú súbor odporúčaní bezprostredne súvisiacich s bezpečnou komunikáciou orgánov verejnej správy na sociálnych sieťach. Sumarizované odporúčania nemusia byť v plnej miere a v celej ich šírke aplikovateľné pre každý konkrétny orgán verejnej správy. Vo všeobecnosti však slúžia ako východisko, aby na základe týchto zásad mohol konkrétny orgán verejnej správy formulovať vlastnú politiku, vlastnú stratégiu a konkrétne prispôsobené štandardy, ktoré zohľadňujú špecifiká danej organizácie. Štandardy by mali byť formulované tak, aby limitovali možnosti misinterpretácie a subjektívneho vnímania úloh, zodpovedností a pridelených rolí. Pri používaní tradičných médií sú v rámci orgánov verejnej správy vytvárané tlačové oddelenia a špecializované pozície hovorcov. Bezpečnej komunikácii na sociálnych sieťach je preto potrebné venovať rovnako patričnú pozornosť.

Každá z desiatich hlavných zásad je dekomponovaná prostredníctvom čiastkových bodov. Dvojstupňové koncipovanie zásad umožňuje konkretizáciu a prispôsobenie konkrétnych politík a stratégií zo strany orgánu verejnej správy tak, aby boli zohľadnené jeho špecifiká, ako napríklad šírka a veľkosť oslovovanej komunity (celonárodné publikum, regionálna alebo lokálna komunita), hierarchia riadenia, charakter orgánu (štátna správa, samospráva), a iné. Komplexnosť orgánov verejnej správy spočívajúca v spravovaní širokého spektra spoločenských situácií v štáte vyžaduje, aby bolo desať zásad bezpečnej komunikácie prispôsobených potrebám konkrétneho orgánu verejnej správy. Napriek tejto komplexnosti je však možné tvrdiť, že zásady sú aplikovateľné na verejnú správu ako celok.

Prezentované desatoro zásad a princípov je možné považovať za súbor odporúčaní, ktoré sa v dnešnej dobe ukazujú ako najdôležitejšie. Nevyhnutné je ale pripustiť a až priam očakávať, že technologický vývoj a ďalší pokrok v oblasti informačno-komunikačných technológií a sociálnych sietí, so sebou prinesie potrebu a nevyhnutnosť reflektovať na nové zásady. Dnešný uhol pohľadu môže len viac alebo menej presne predpovedať budúci vývoj a nové výzvy bezpečnej komunikácie orgánov verejnej správy. Osobitný zreteľ by ale mal byť venovaný integrácii umelej inteligencie a chatbotov, automatizovaným nástrojom na generovanie a prezentovanie obsahu, ale aj využívaniu digitálnych osôb a avatarov generovaných prostredníctvom umelej inteligencie ako hovorcov / hovorkýň orgánov verejnej správy.

Miera zodpovednosti orgánov verejnej správy za kvalitu informácií vo verejnom priestore narastá, pretože pridaná hodnota informácií podaných orgánom verejnej správy je z pohľadu občana alebo podnikateľského subjektu oveľa vyššia, nakoľko ovplyvňuje práva, povinnosti a právom chránené záujmy dotknutých subjektov.