

# Zvyšování odolnosti státní správy proti nelegitimnímu ovlivňování

4



audit národní  
bezpečnosti

Audit národní bezpečnosti schválený usnesením vlády č. 1125 ze dne 14. prosince 2016<sup>1)</sup> popsal deset hlavních bezpečnostních hrozeb pro Českou republiku, přičemž jednou z nich je tzv. „**působení cizí moci**“. Na základě doporučení Auditů probíhá od roku 2018 školení vybraných státních zaměstnanců a dalších zaměstnanců veřejné správy zaměřené na zodolnění vůči pokusům o nelegitimní ovlivňování, které pořádá Ministerstvo vnitra spolu se zpravodajskými službami (Bezpečnostní informační službou a Úřadem pro zahraniční styky a informace). Svým usnesením č. 794 z 25. října 2023 vláda České republiky rozhodla o pokračování těchto školení.

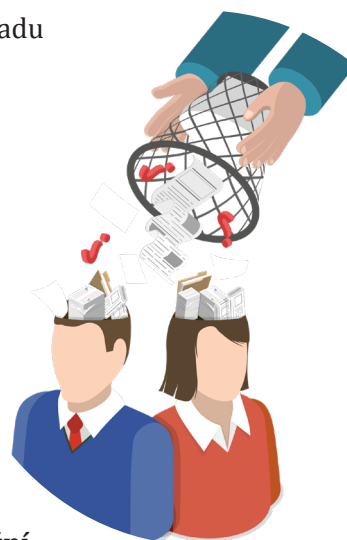
Většina těchto zaměstnanců absolvuje toto školení formou e-learningu. Ti, kteří mají přístup k většímu množství citlivých informací anebo disponují zvýšenými rozhodovacími pravomocemi, mohou být na základě rozhodnutí služebního orgánu vysláni na školení prezenční.

## CO TO JE NELEGITIMNÍ OVLIVŇOVÁNÍ

Nelegitimní ovlivňování je souhrnné označení pro celou řadu zpravidla cílených aktivit a činností, které jsou svojí povahou protiprávní anebo nežádoucí. Původcem nelegitimního ovlivňování je útočník, který se všemi jemu dostupnými prostředky snaží o prosazení svých zájmů, a to tak, že pomocí svého aktivního jednání zasahuje do zájmů někoho jiného (cíle nelegitimního ovlivňování).



Nelegitimní ovlivňování je **nežádoucí působení na lidi, rozhodování, či procesy**. Zahrnuje jak vlivové působení cizí moci,<sup>2)</sup> tak i kriminální (např. korupční) jednání a nežádoucí lobbování. **Obvykle jde o aktivity, které jsou skryté, klamavé, vynucující či korupční,** a které útočník (cizí moc, korupčník, lobbista postupující v rozporu se



nelegitimní  
ovlivňování

definice

<sup>1)</sup> Podrobnosti k Auditů národní bezpečnosti viz <https://www.mvcr.cz/chh/soubor/audit-narodni-bezpecnosti.aspx>

<sup>2)</sup> Český právní řád obsahuje definici pojmu „cizí moc“ v zákoně č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů v § 2, písm. g) takto: „Cizí mocí se rozumí cizí stát nebo jeho orgán anebo nadnárodní nebo mezinárodní organizace nebo její orgán.“ Pro účely tohoto textu definici rozšíříme i o jakékoliv další fyzické osoby bez ohledu na jejich státní příslušnost, či právnické osoby bez ohledu na jejich sídlo anebo místo působení, pokud se podílí, byť i jen částečně, na prosazování zájmů cizí moci formou nelegitimního ovlivňování.za

zákonem, případně obecně uznávanými společenskými etickými pravidly) vykonává **sám anebo prostřednictvím třetí strany**, a které **ohrožují či poškozují naše zájmy**.

## TÝKÁ SE STÁTNÍCH ZAMĚSTNANCŮ NELEGITIMNÍ OVLIVŇOVÁNÍ?

Ano týká. **Existují subjekty prosazující svoje zájmy v rozporu s demokratickými principy, právním řádem**, ale i dobrými mravy, a ty v tomto kontextu označujeme za útočníky.

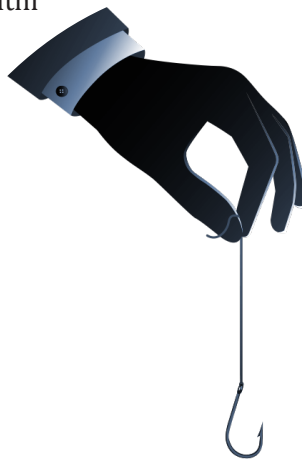
Útočníci se snaží najít co možná nejjednodušší cestu

k prosazování svých zájmů, přičemž v absolutní

většině případů takové aktivity směřují

vůči nějaké fyzické osobě (v tomto

případě státnímu zaměstnanci).



Celá řada státních zaměstnanců

(a nejen jich) má dojem, že

jejich práce je pro jiné osoby

(potenciální útočníky)

nezajímavá, nemá přístup

k informacím, které by mohly

být pro někoho zajímavé nebo

mít nějakou hodnotu, a že nemá

žádnou anebo jen minimální

rozhodovací pravomoc. Takové

přesvědčení je ale nesprávné,

a naopak zvyšuje pravděpodobnost

úspěchu útočníka, pokud svoje zájmy

zkusí prosazovat právě prostřednictvím

fyzické osoby, která je přesvědčená, že je pro

potenciálního útočníka nezajímavá. Právě u takového člověka

je vysoká pravděpodobnost, že signály naznačující, že by mohl být cílem nelegitimního ovlivňování, přehlédne, nebo je bude podceňovat.



V konečném důsledku může takový přístup a nesprávná nebo žádná reakce státního zaměstnance na nelegitimní ovlivňování či pokus o něj způsobit poškození politických, ekonomických, bezpečnostních, reputačních, ale i dalších zájmů České republiky.

Je třeba si uvědomit, že kterýkoli státní zaměstnanec **se může stát cílem nelegitimního ovlivňování kvůli tomu:**

- » **K čemu má přístup** – přichází do styku s různými interními dokumenty, pracuje s databázemi obsahujícími osobní údaje či jiné citlivé anebo interní informace; má interní informace vztahující se k zadávání veřejných zakázek, má přístup k interní počítačové síti apod.

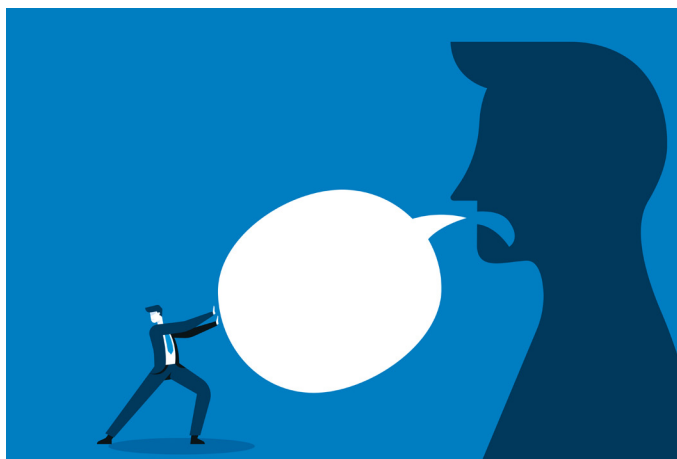
státní zaměstnanec  
jakožto cíl  
nelegitimního  
ovlivňování

- » **Kam má přístup** – jako zaměstnanec má fyzický přístup do prostor, kam nemůže veřejnost, v některých případech i do míst, kam nesmí ani většina dalších zaměstnanců úřadu; umí popsat bezpečnostní opatření fyzické, administrativní, ale i režimové povahy
- » **Ke komu má přístup** – nejde jen o kolegy, ale i představené a zaměstnance jiných úřadů a dalších státních i nestátních subjektů, se kterými spolupracuje
- » **Co ví** – je schopen popsat dynamiku vztahů na pracovišti, ví kdo má přístup k jakým informacím anebo do jakých prostor, zná řadu velice osobních informací o lidech, se kterými spolupracuje

V některých případech nemusí být cílem přímo konkrétní státní zaměstnanec, ale může se stát nástrojem útočníka k ovlivňování někoho jiného, tj. třetí osoby či subjektu.

## JAK NELEGITIMNÍ OVLIVŇOVÁNÍ ROZPOZNAT A JAK POSTUPOVAT

Identifikace jednotlivých forem a metod útoku a způsobu obrany proti nim se v zásadě neliší podle toho, zda je útočníkem zástupce cizí moci, korupčník či lobbista postupující v rozporu se zákony či dobrými mravy. Aktérem útoku je vždy „člověk“, bez ohledu na to, zda jedná sám či ve prospěch nějakého státu, firmy, organizace apod. Je tak velmi pravděpodobné, že v absolutní většině případů se útočník, stejně jako každý jiný člověk, dopustí řady větších či menších chyb, kterých si lze všimnout.



Zkušenosti ze zjištěných případů nelegitimního ovlivňování, ať již u nás anebo v zahraničí, ukazují, že v absolutní většině případů bylo lidem, kteří se stali cílem nelegitimního ovlivňování či jejich nejbližšímu okolí, zcela zřejmé, že **je „něco špatné“, případně „jinak“, než je v obdobných situacích běžné.**

Pokud má zaměstnanec pocit, že se děje něco zvláštního, podivného, či se někdo v nějaké situaci chová či jedná neodpovídajícím způsobem, **je vhodné informovat svého představeného či odpovědného zaměstnance bezpečnostního odboru/oddělení úřadu** a konkrétní podezření s ním prodiskutovat. V krajním případě je pak možné obrátit se cestou e-mailu [prevence@bis.cz](mailto:prevence@bis.cz) přímo na Bezpečnostní informační službu.

Bezprostředně nadřízený představený či zaměstnanec bezpečnostního odboru/oddělení se státním zaměstnancem podezření prodiskutuje a navrhne další postup. V některých případech se může rozhodnout, že bude vhodné informovat o celé situaci i Policii České republiky či Bezpečnostní informační službu.

postup při podezření

## JE NUTNÉ ZJIŠŤOVAT KDO JE ÚTOČNÍKEM?

Nehraje roli, zda je útočníkem cizí moc, nějaká kriminální skupina snažící se např. korupčními aktivitami přimět zaměstnance k tomu, aby nějakým způsobem konal, či někdo jiný. Důležité je, nenechat si informaci o možném probíhajícím pokusu o nelegitimní ovlivňování pro sebe.

Pro správné vyhodnocení konkrétní situace, v níž může docházet k nelegitimnímu ovlivňování, je velmi užitečné, zapamatovat si co možná největší množství detailů, které by mohly pomoci odpovědět na šest základních otázek: Kdo? Co? Kdy? Kde? Jak? a Proč?

hlavní zásady

## HLAVNÍ ZÁSADY

### TŘI PILÍŘE PRO ZVÝŠENÍ ODOLNOSTI

**I.**

každý má přístup k citlivým informacím, které se mohou stát cílem zájmu útočníka (jinými slovy: informace, které jsou pro někoho bezcenné, mohou mít velkou cenu pro někoho jiného)

**II.**

každý se může stát předmětem zájmu (nelegitimního ovlivňování) - rozhodnutí, zda se zaměří přímo na zaměstnance, je na útočníkovi, zaměstnanec sám jej nemůže nijak ovlivnit

**III.**

každý se může bránit - jsou k dispozici nástroje, jak nelegitimní ovlivňování rozeznat a jak se v takových situacích zachovat => každý se může na někoho obrátit