

PODKLAD NA JEDNÁNÍ ZASTUPITELSTVA DNE 1. 10. 2026

Věc: kybernetický útok na počítačový systém obce - informace starosty

Starosta obce informoval zastupitelstvo o kybernetickém incidentu, který se uskutečnil v polovině loňského roku, když uvedl, že informuje ZO až nyní, tj. po té, co bylo šetření tohoto kybernetického incidentu orgány Policie ČR pravomocně ukončeno, a pominula tak jeho mlčenlivost v souvislosti s probíhajícím šetřením.

1/ Základní informace - na vědomí:

- dne 2.6. 2025 starosta zjistil, že při přihlášení do ekonomického systému obce systém nefunguje, nelze se řádně přihlásit, a na stránkách je umístěn anglicky psaný text.

- obratem byl kontaktován externí správce sítí úřadu IT specialista Ing. Viktor Trnka a po jeho prověrce bylo konstatováno, že v neděli 1.6. 2025 v nočních hodinách byl server obce napaden, a speciálním systémem byla umístěná data během noci zašifrována a zanechán vzkaz co se stalo a jakým způsobem se může k takto zašifrovaným datům obec dostat, s tím, že jako příčina vzniklé situace bylo s největší pravděpodobností stanoveno, že došlo k „prolomení hesla“ externí účetní pro práci ze vzdáleného přístupu,

- bezprostředně byl IT technikem deaktivován napadený vzdálený přístup a došlo ke změně hesel na všech počítačích. Současně byl tento kybernetický incident oznámen starostou pověřenci GDPR a Policii ČR a ta jej bezprostředně již 3.6. 2025 kontaktovala a bylo zahájeno šetření ve věci, když ve věci podával vysvětlení jak starosta, tak i Ing. Trnka, když oba byli zavázáni mlčenlivostí. Policie ČR pak byla v průběhu šetření informována o všech krocích, které obec za pomoci svého správce sítí činila ke zjednání nápravy,

- bezprostřední prověrkou stavu sítě provedenou Ing. Trnkou bylo zjištěno, že úřad za tohoto stavu není schopen ve stávající režimu fungovat, zneužití dat či napadení účtů obce nebylo zaznamenáno, přičemž náklady na znovuobnovení programů, sítě zabezpečení apod., byly v této době odhadovány na částku cca 1,5 mil. Kč, a tato částka také byla sdělena Policii ČR,

- za této aktuálně „bezvýchodné“ situace doporučil správce sítě pokusit se reagovat na komunikaci pachatele, a po souhlasu starosty ve své režii a v rámci svého zabezpečení a svého PC reagoval na anglicky psaný text se žádostí o sdělení, za jakých podmínek by bylo možné dešifrování souborů, na což pachatel reagoval tím, že po zaplacení 2000,- EUR s platbou v Bitcoinech. Po vyhodnocení stavu, rizik i případných nákladů na znovuobnovení systému, na to bylo přistoupeno, a tato částka byla Ing. Trnkou z jeho prostředků uhrazena. O všech těchto úkonech i komunikaci s pachatelem útoku včetně zaplacení uvedené částky požadovaným způsobem byla Policie ČR v rámci šetření průběžně informována, byla ji předávána příslušná komunikace, včetně platebních dispozic, a veškeré tyto okolnosti jsou zaznamenány ve spisu Policie i v konečné rozhodnutí Policie ČR ve věci,

- po zaplacení uvedené částky 2.000,- EUR obdržel Ing. Trnka dešifrovací program, který po ověření na vybraných vzorcích, umožnil obnovení dat do původní podoby, všechny počítače a veškerá data byla prověřena dvěma antivirovými programy, zda se napadení nemůže opakovat, a byl tak obnoven systém do původní podoby, přičemž nebyl zaznamenán žádný únik umístěných dat, přičemž šetření věci Policií ČR dále pokračovalo,

- ze šetření Policie ČR mj. vyplynulo, že se nepodařilo zjistit zařízení, ze kterého byl proveden vzdálený přístup, a v rámci šetření finanční transakce zaplacení 2.000,- EUR se ani nepodařilo zjistit koncového uživatele či majitele krypto peněženky. Z těchto důvodů bylo šetření ukončeno a trestní věc vedená proti neznámému pachateli odložena, neboť se nepodařilo zjistit skutečnosti, které by opravňovali konat proti určité osobě. Z vydaného policejního rozhodnutí – Usnesení Policie ČR, KŘP Lib. kraje, odd. kybernetické kriminality, pak mj. rovněž vyplývá, že se nejednalo o jediný incident, když neznámý pachatel se takto pokoušel připojit i např. do sítě Obecního úřadu Benátky nad Jizerou, i dodavatele softwaru Triada,

- na základě tohoto incidentu byla obcí bezodkladně po tomto incidentu, a následně i po obnovení dat přijata a realizována opatření k nápravě způsobem, jak byla navržena správce sítě Ing. V. Trnkou, jež by měla podobným incidentům lépe bránit, mimo jiné byl zřízen jiný způsob připojování pomocí šifrovaného OpenVPN, hesla se již nikde neukládají a budou se pravidelně měnit. Kromě pravidelného denního online zálohování na NAS se budou provádět i offline zálohy na externí disk uložený v trezoru,

-po vyhodnocení bylo konstatováno, že se nejednalo o cílený útok na obec Malá Skála, ale zcela náhodný a sofistikovaný hackerský útok vedený proti řadě subjektů s využitím možnosti „prolomení konkrétního hesla“, a s ohledem na možné dopady a případné ohrožení činnosti obce, ale i výsledky šetření Policie ČR, kdy se nepodařilo dohledat stopy tohoto útoku, se ukázala realizovaná opatření jako v daném případě nejvhodnější,

2/ Návrh na vypořádání nákladů:

Za tohoto stavu se navrhuje, aby ZO na základě provedené informace starosty vzalo tuto informaci na vědomí a schválilo navržené vypořádání vynaložených nákladů a odměny ze strany správce sítí, když :

-náklady na řešení kritického stavu po incidentu nesl správce sítí, který také požadovanou „částku za dešifraci“ 2.000,- EUR, tj. 52.557,-Kč, zaplatil ze svých prostředků dne 3.6.2025,

-náklady IT specialisty Ing. Trnky za účast na řešení případu, odšifrování, zálohování, stanovení nových hesel, kvalitnějšího zabezpečení je vyčísleno v rozsahu 50 hodin práce, tj. ve výši 50.000,- Kč.

3/ Návrh usnesení

- ZO bere informaci ohledně kybernetického incidentu a přijatých opatření k nápravě na vědomí

- Schvaluje návrh na vypořádání nákladů vynaložených správce sítě na odstranění vzniklé situace a zpracování podkladů k nápravě a zajištění kybernetické bezpečnosti systému obce.