Kybernetický útok není strašák pro korporace, ale realita i pro „Lhotu“. Náměšť nad Oslavou je jen špičkou ledovce

24.4.2026 - | Sdružení místních samospráv ČR

Hackerský útok na radnici v Náměšti nad Oslavou 1. dubna opět otevřel otázku, jak jsou české obce připraveny na digitální hrozby. Mnoho starostů se domnívá, že pro hackery nejsou zajímaví, opak je ale pravdou – jsou nejsnazším cílem.

Jak zabezpečit obec i s minimálním rozpočtem a bez vlastního IT týmu? Pavel „Spajk“ Matějíček v kuloárech krajských shromáždění SMS ČR radí starostům jasně: *„Nezačínejte nákupem drahých krabic, začněte inventurou a jednou stránkou A4 s krizovým plánem.“*

Starosta malé obce má na stole tisíc priorit – od odpadů po dotace na školku. Proč by měl věnovat čas a peníze zrovna kyberbezpečnosti? Je to skutečně reálná hrozba pro ‚Lhotu‘, nebo jen strašák pro velké korporace?

Protože obec dnes není jen úřad s razítkem, ale taky malá digitální firma. Má e-maily, účetnictví, spisovou službu, Czech POINT, osobní údaje občanů, komunikaci se školou, technickými službami i dodavateli. A útočníkovi je v zásadě jedno, jestli útočí na ministerstvo nebo na Lhotu. On si nevybírá podle velikosti obce, ale podle toho, kdo je nejsnazší cíl.

U malé obce bývá problém právě v tom, že nemá vlastní IT tým, všechno často stojí na jednom správci nebo externistovi a bezpečnost se odsouvá, protože „teď hoří něco jiného“. Jenže kyberútok pak neznamená jen problém pro počítače. Znamená zavřený úřad, nedostupné dokumenty, výpadek služeb a často i dost drahou obnovu. Takže kyberbezpečnost není luxus navíc. Je to dnes stejná základní provozní povinnost jako zamykat budovu nebo mít pojištění.

Tady jeden aktuální případ:
https://brnensky.denik.cz/zpravy_region/zidlochovice-hackeri-kyberneticky-utok-vykupne-data-software-ransomware-kldr.html

V poslední době objíždíte krajská shromáždění SMS ČR a mluvíte s řadou starostů a starostek. Co je ta jedna věc, u které vidíte, že je pálí nejvíc? A co jim v kuloárech radíte jako úplně první krok, když za vámi přijdou s obavou: ‚My na to IT nikoho nemáme, co máme vlastně dělat?

Nejčastější obava je úplně jednoduchá: *„My na to nikoho nemáme.“* A s tím souvisí druhá věta: *„My vlastně ani nevíme, co všechno máme chránit.“* To je podle mě ještě častější.

A tady je jádro problému. Ne že by starostové byli lehkomyslní. Spíš často nevědí, kde začít, a mají pocit, že kyberbezpečnost je drahá, složitá a jen pro velké organizace.

V kuloárech jim říkám jako první věc: nezačínejte technologiemi, začněte přehledem. Sepište si tři jednoduché seznamy: co všechno v obci používáte za systémy a služby, kdo k nim má přístup a kdo je za co odpovědný. V tu chvíli totiž většina obcí zjistí, že nemá problém jen s bezpečností, ale už i s pořádkem. A bez pořádku nejde dělat bezpečnost.

Druhý krok je ověřit, jestli máte funkční zálohy a jestli je umíte obnovit. A třetí krok je nastavit úplné minimum: silná hesla, vícefaktorové ověření, aktualizace a jasný kontakt na někoho, komu se volá při

incidentu. To je mnohem důležitější než nakoupit drahou krabici, které nikdo nerozumí.

Představme si černý scénář: Starosta přijde do práce, zapne počítač a tam svítí nápis, že jsou všechna data zašifrovaná a úřad chce výkupné. Co má v tu první minutu udělat?

V první minutě platí jediné: zastavit šíření a nepanikařit.

To znamená:
odpojit napadený počítač od sítě a internetu, nevypínat ho ukvapeně, neklikat dál na nic podezřelého a okamžitě dát vědět vedení, IT správci nebo dodavateli. Když obec nikoho takového nemá, je potřeba co nejrychleji aktivovat někoho, kdo incident převezme odborně – jsou na to specializované firmy.

Co naopak rozhodně nedělat?

Neplatit hned výkupné, nesnažit se to „nějak proklikat“, nemažte stopy a nezačínejte chaoticky přepojovat ostatní počítače. Úplně nejhorší je dělat, že se nic nestalo, a doufat, že to samo zmizí – i to jsme viděli. V tu chvíli totiž běží čas a útok se může šířit dál.

Prakticky bych to vzal takto: izolovat zařízení, zachovat důkazy, ověřit, co je zasažené, a spustit incidentní postup. Kdo má připravený jednoduchý krizový scénář, ten je v obrovské výhodě. Kdo ho nemá, ten ho začíná psát ve chvíli, kdy už hoří.

…

Celý rozhovor s panem Matějíčkem si můžete pročíst v dubnovém vydání zpravodaje SMSka. Celé číslo si přečtete v elektronické podobě zde. Archiv s předchozími vydáními si otevřete zde.

https://www.smscr.cz/o-sms-cr/aktuality/kyberneticky-utok-neni-strasak-pro-korporace-ale-realita-i-pro-lhotu-namest-nad-oslavou-je-jen-spickou-ledovce-5227cs.html