

Všechny instituce Nového Města na Moravě jsou nyní v bezpečí



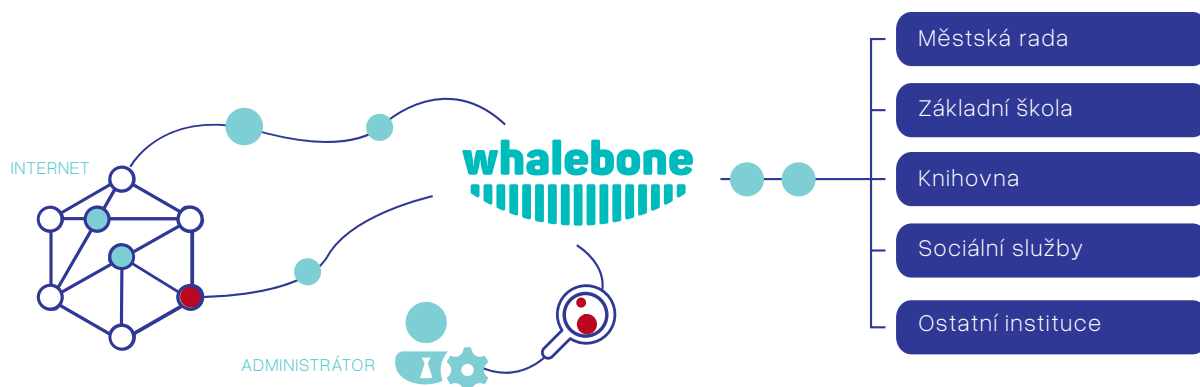
„Bez tohoto stupně
ochrany si už jako
systémový správce
nedovedu provoz na síti
představit. Jen mě mrzí,
že jsme ho nezačali
využívat dřív.“

ZBYNĚK GREPL
VEDOUcí ODDĚLENÍ
INFORMATIKY MĚSTA



Výzva

Whalebone je ideální řešení pro města a regiony



Jen v roce 2020 proběhlo přes 300 kybernetických útoků na český veřejný sektor. Po nemocnici v Benešově (na měsíc vyřazena z provozu, škody v desítkách miliónů) to byla nemocnice v Brně–Bohunicích, magistrát v Olomouci i v Praze.

Jedním z českých měst, které se už kyberútoků nemusí bát, je

Nové Město na Moravě, které do své bezpečnostní infrastruktury zahrnuje i ochranu na úrovni DNS od Whalebone.

Veřejné instituce – městský úřad, příspěvkové organizace, školy, lázně, sociální a technické služby – tak nejsou ohroženy cílenými kyberútoky ani náhodnou infiltrací malware, spyware nebo ransomware.

Whalebone je ochrana na síťové úrovni, takže přesměrováním provozu dokážete pokrýt všechny instituce, které máte ve správě.

Kromě zásadní ochrany a toho, že administrátoři získají přehled o všem, co se v síti děje, vám Whalebone umožní nastavovat různé politiky pro jednotlivé instituce, například podle proškolenosti uživatelů.

Nejedno české město se chlubí tím, jak má jedinečně zachovalé hradby – a nevědomky tak přiznávají, že poslední doba, kdy měla skutečně funkční ochranu před nepřítelem na úrovni své doby, byl středověk.



Řešení

3 důvody, proč Nové Město na Moravě zvolilo Whalebone



Snadné uvedení do provozu

Bez nutnosti instalace. Pohyby směrem do sítě se filtrují přes DNS resolvers, na které je potřeba se pouze přesměrovat, nikoli je složitě integrovat a následně o ně pečovat.



Dokonalý přehled

Přesný přehled o tom, jaké konkrétní útoky systém odrazil. Z možných nastavení se rozhodli pro týdenní zasílání reportů, je ale možné sledovat „boj na hradbách“ v reálném čase.



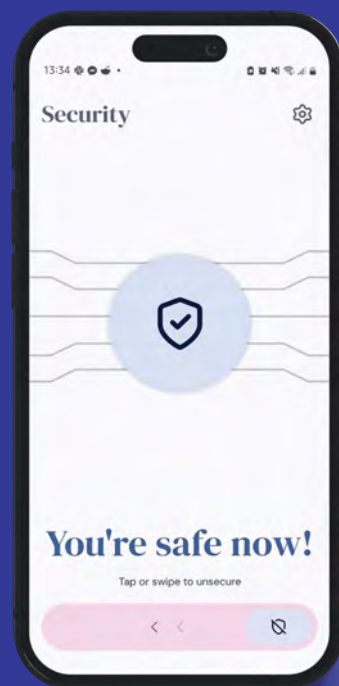
Bezzásahový provoz

Immunity nepotřebuje neustálou obsluhu. Případně se řeší pouze jednotlivé poplašné zprávy, které Whalebone posílá na síťový helpdesk.

„Nikdy dřív jsem se nesetkal s ničím, co bych do deseti minut aktivoval a ono to fungovalo.“

„U firem a organizací, které znám, jsem si ověřil, že to funguje. Někupujeme zajíce v pytli.“

ZBYNĚK GREPL,
VEDOUcí ODDĚLENÍ INFORMATIKY MĚSTA



Výhody

Jak Whalebone chrání Nové Město na Moravě

Jakýkoli uživatel zařízení spadajícího do městské sítě (zaměstnanec se služebním telefonem, žák na školním počítači apod.) už nemůže způsobit ohrožení, protože DNS ochrana blokuje rizikové domény.

Jednoznačným přínosem oproti jiným řešením je možnost identifikovat konkrétní zařízení, přes které riziko přichází, zmapovat jeho činnost a okamžitě zařídit nápravu.

Nejde však jen o zařízení v městské správě. Whalebone například odhalil nebezpečný přístroj externího uživatele, který se napojil do městské sítě.

Správce proto omezil možnost dynamického připojování dalších zařízení přes DHCP a aktuálně je nutné o něj vždy požádat.

Whalebone chrání
významné instituce
veřejné správy v Česku
i na Slovensku



NAŠI ZÁKAZNÍCI



Jednoduše přesměrujte
traffic z vaší sítě na
resolvery Whalebone
a zahajte bezplatnou
zkušební verzi.

immunity@whalebone.io

Rádi vám odpovíme na všechny otázky.
Naším hlavním cílem je oboustranná
spokojenost – uděláme vše pro to,
abychom vám vyhověli.

www.whalebone.io

Více o našich produktech najdete
na: whalebone.io/immunity

Píče informací o DNS zabezpečení
sledujte náš LinkedIn.