whalebone

Case study
Nové Město na Moravě

NM
NM

I can no longer imagine running a network without this level of security. My only regret is not having started to use it sooner.”

Zbyněk Grepl,
Director of the Municipal IT Department

All institutions of Nové Město na Moravě are now secure

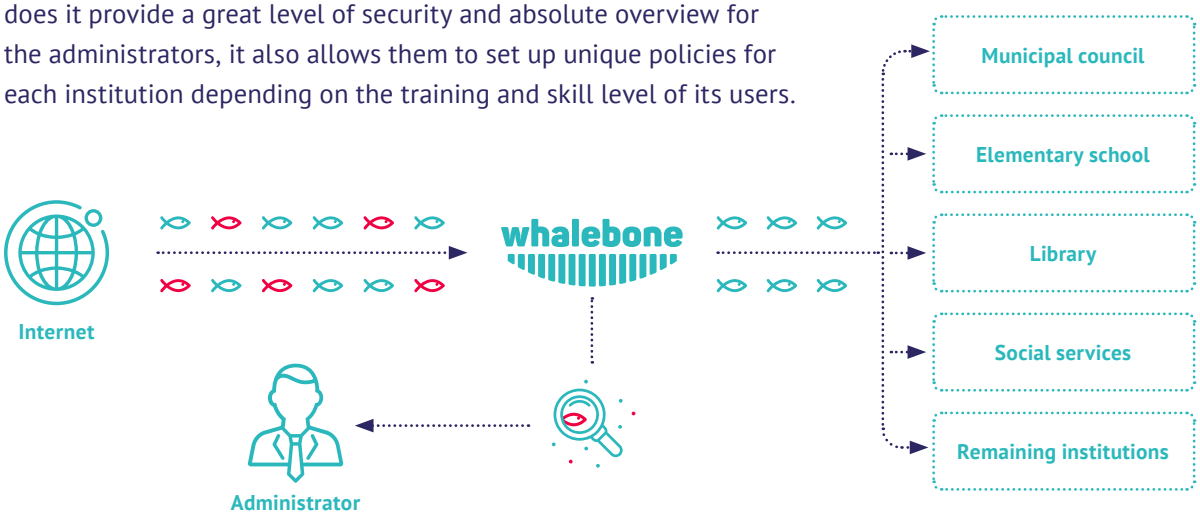
Many Czech cities are proudly presenting their medieval walls and gates – unknowingly admitting that the last time their city was actually secure from current threats was during the Middle Ages.

There had been over 300 cyberattacks aimed at Czech institutions in the public sector in 2020. Benešov hospital was put out of service for over a month inflicting damages in tens of millions. Brno-Bohunice hospital and municipal councils in Olomouc and Prague met similar fate.

A town that does not have to be afraid of such attacks anymore is Nové Město na Moravě as it implemented Whalebone Immunity into their security infrastructure. Public institutions such as the city council, public institutions, schools, spas or social services are no longer in danger of cyberattacks, malware, spyware or ransomware infiltration.

Whalebone is a great solution for cities and regions

Whalebone runs on the level of network security and by redirecting traffic it facilitates protection for all the institutions at once. Not only does it provide a great level of security and absolute overview for the administrators, it also allows them to set up unique policies for each institution depending on the training and skill level of its users.



4 reasons why Nové Město na Moravě chose Whalebone

1 Extremely easy implementation

without any installation. Incoming and outgoing network traffic is filtered through DNS resolvers. No complicated installation or maintenance of the resolvers is needed as the traffic is simply forwarded to Whalebone Resolvers.

I've never come across any other product that gets implemented in ten minutes and simply works.

Zbyněk Grepl,
Director of the Municipal IT Department

2 Absolute overview

of all the attacks that had been deflected by the system. The IT department of Nové Město na Moravě chose a weekly report option but it is possible to spectate the defence in real time.

3 Uninterrupted service

that does not require permanent staffing. Occasional alerts are sent the network helpdesk.

4 Great references

from organizations I personally know and work with. Thanks to their feedback I knew that we were not buying a pig in a poke.

Zbyněk Grepl

All users using devices connected to the municipal network (such as officials with business phones or students using the school computer) can no longer put the whole network in danger as the DNS security blocks all unsafe domains. One of the main advantages over other solutions is tracing down the specific device that is causing the threat, easily monitoring it and removing the problem.

Municipal devices are not the only ones being monitored. For example, Immunity detected a dangerous device of an external user who was connected to the municipal network. Following this, the administrator restricted the dynamic DNS connection through DHCP for all devices and no user can use it without making a request.

Reception of the system amongst employees?

Employees got used to the fact that if they are denied access to a certain page the system explains why. Whalebone only blocks domains with higher risk than is the set threshold. The intuitive threshold score can be manually adjusted for each institution by administrators – for example school or public computer's threshold can be more strict than the one of business phones. The policies can be easily adjusted in our portal. Certain domains can be put on a whitelist. There is also the option to add a "proceed to an unsafe page" button to the blocked page.

Feedback of the network administrator

"I can no longer imagine running a network without this level of security. My only regret is not having started to use it sooner."
It is clear as day that recent cyberattacks aimed at main cities and key institutions were deliberate and did not occur randomly. Most common threats for the municipality of this size, however, are rather unaddressed malware or spyware threats and random phishing schemes. Nevertheless, those threats can cause serious problems anyway. Sustainable and reliable prevention of cyber attacks that can be used whenever and wherever should be a part of strategic plan of every responsible municipal council.

Whalebone protects key institutions of public service in the Czech Republic and Slovakia

Additional references

Easily redirect part of your network traffic to Whalebone resolvers and try out our trial.

sales@whalebone.io

Learn more about our product at whalebone.io/cs/corporate, ask for a demo version or contact us via e-mail.

www.whalebone.io

We will be more than happy to answer any questions. Mutual satisfaction is our main goal and we will do our best to fulfil your requests.