Unauthorized access control in water utility computer networks

Ioan Florin VOICU,
ING Hubs, Bucharest, Romania
ioan-florin.voicu@ing.com

Dragos Cristian DIACONU,
Bucharest University of Economic Studies, Bucharest, Romania
diaconudragos23@stud.ase.ro

Daniel Constantin DIACONU,
University of Bucharest, Bucharest, Romania
daniel.diaconu@unibuc.ro

Abstract
Virtual tampering in water utility systems can lead to highly dangerous real-world situations such as shortages and permanent damage to infrastructure. While cybersecurity guidelines do exist for Romanian companies like ApaNova, they are inadequate for protecting the water supply chain. Evaluating the potential vulnerabilities such systems have and presenting open-source methods to improve them is critical for the cybersecurity sustainability of utility services. Building on previous research regarding network cybersecurity, Kali Linux was used as a penetration testing platform in conjunction with an OPNSense-based network configuration. Initially the test included just the Apa Nova-mandated security settings (focusing on ransomware & database access protection), after which additional protective layers were added. The first extra layer was VLAN network segmentation, in compliance with Environmental Protection Agency (EPA)'s America's Water Infrastructure Act (AWIA) guidelines. Afterwards, additional settings were added, such as: Intrusion Detection Systems (IDS) & Intrusion Prevention Systems (IPS); Employee access only via Virtual Private Network (VPN) and Medium Access Control (MAC) address filtering for all employee Wi-Fi devices. A monitoring solution in OPNSense was also implemented, in order to be informed of any suspicious activity on the network. In conjunction with this, a patching strategy was created, which would minimize downtime, while ensuring the system is kept up to date. This is facilitated by the open-source nature of OPNSense, which does not need costly license upgrades to remain secure. The results showed that while protection against ransomware/viruses is important and relatively easy to implement, testing confirmed the findings of previous articles that malicious internal actors are an even greater threat than viruses. This requires constant protection and monitoring against privilege misuse by even authorized personnel. A wider view is offered on how easy it is to gain access to current systems and several off-the-shelf open-source software solutions are highlighted that can prevent water utility shutdown or misuse by malicious actors.

Keywords: Pen Testing, OPNSense, VPN, water management.

1. Introduction
Due to current private & state-sponsored hacking attempts on water, power & other such utility infrastructure, it's become ever more important to protect these assets from unauthorized remote access and ensure that any virtual threat is dealt with proactively by proper server patching & employee access procedures.

The hypothesis of this case study is that a water utility network with minimal cybersecurity infrastructure is relatively easy to penetrate by malicious actors and adding extra layers of network & authorization security greatly increases the difficulty of unauthorized access.

Whereas in the past obtaining proper network security required expensive licenses and specialized hardware, open-source projects such as OPNSense have lowered the cost and complexity of obtaining such benefits, while virtual machine platforms like Proxmox VE have enabled easier configuration and improved uptime for any of the operating systems it hosts.

Such platforms have standardized both the testing & roll-out of necessary systems, while ethical hacking Linux distributions like Kali have enhanced the capabilities and ease of penetration testing, which has been proven to improve the overall security evaluation of Wi-Fi networks [1].

Notable is also the fact that with newer hardware and OPNSense being able to use regular x86 processor platforms, the cost and performance penalty of IDS & IPS protection has significantly decreased, making enabling it less of a tradeoff than in previous years [2]. It is also important, however, to calibrate the monitoring & alerting capabilities appropriately to not have either "notification overload" or miss potentially important network events [3].

Ultimately, though, the security culture of the utility company is one of the best guarantors of its continued proper operation, with the incident and reputational cost of not applying best practices in this field far outweighing the occasional operational savings that could be made. This is especially important for smaller water utility operators, that may have an oversized impact, but do not have enough resources allocated for such purposes [4]. Open-source software would be an ideal way for these operators to have a widely-supported security infrastructure with crowdsourced threat identification.

2. Methodology

This case study attempted to simulate on a small scale the computer network layout of a water utility provider, creating a complete sample network infrastructure, as well as ways to access this infrastructure both locally and remotely.

The attempts to access the infrastructure initially mimicked the behavior of company employee devices, in order to not trigger anti-malware systems within the network.

The ease of unauthorized access was then compared at each step during the addition of multiple extra layers of security. The network thus progressed from being relatively trivial to penetrate from a nearby physical location to requiring separate VPN access rights, blocking access to the most critical areas by default and triggering the IDS/IPS notifications that had been added.

Just as importantly, the patching & downtime strategy that was implemented led to a significant increase in planned availability and a reduction in the number of downtime-causing incidents.

2.1. Case Study Hardware Setup

For this case study there needed to be several virtual servers, a Wi-Fi access point, a PC operating system client and a mobile operating system client. The choices made in terms of hardware were:

- An Intel Core i5 (7th generation) server/router/firewall with virtual machine support & 2 network cards
- A Ubiquiti Unifi AC Pro Wi-Fi access point
- A Lenovo ThinkPad T480 for both wired & Wi-Fi access from a PC operating system
- A Google Pixel 7 device for both Wi-Fi & 5G access from a mobile operating system

2.2. Case Study Software Setup

In terms of software setup, the architecture was designed around a server running Proxmox VE. This server would be the host for multiple virtual machines. One of these virtual machines was running OPNSense for router/DHCP/firewall/VPN duties, another was running the Unifi Network application for Wi-Fi access point management, while yet another was the target utility company application server for pen testing/exploiting, running the latest version of Ubuntu Server. The VPN plugin that was used in OPNSense was Wireguard, widely seen as the best-performing open-source VPN solution currently available.

For pen testing, the mobile ThinkPad T480 machine was used, running Kali Linux, the standard Linux distribution for such purposes. The machine's mobility allowed for testing the effectiveness of the security measures both in physical proximity to the simulated utility company's offices, as well as from within the network itself.
The testing was done as a multi-tier process, as the utility company's software defenses were also ramped up.

Initially, the testing was performed with a regular Unifi Wi-Fi configuration, with no MAC filtering & a shared WPA2 Wi-Fi access password. This was then enhanced to a Wi-Fi configuration with MAC filtering that only allowed all known employee devices.

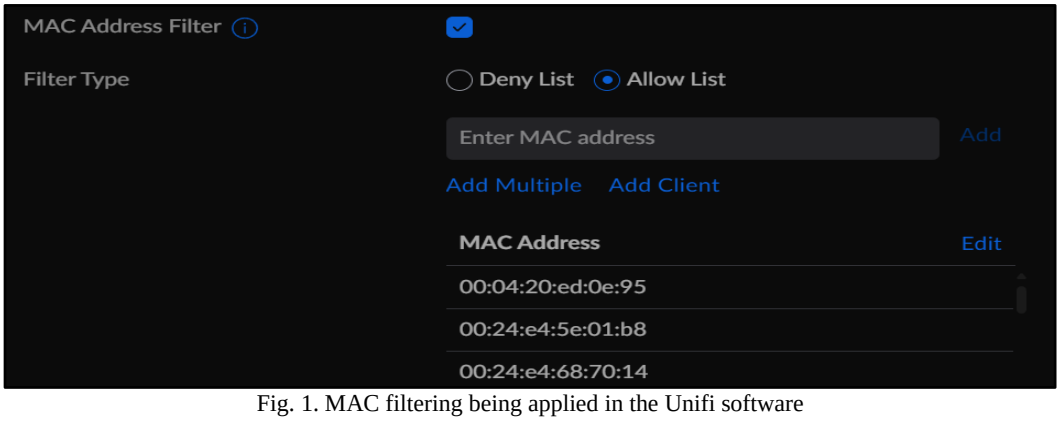

Fig. 1. MAC filtering being applied in the Unifi software
Source: author's testing

After the wireless pen testing results were obtained, OPNSense was deployed as a router, DHCP server & firewall. The first stage was without VLAN traffic separation, after which VLANs were created for the employee & server infrastructure networks.

This still allowed for unencrypted remote access, so a VPN solution was installed and made mandatory for all mobile employee devices.

The next stage after securing access was to monitor network traffic, for which OPNSense has a Suricata-based solution for IDS/IPS. To implement this, appropriate rule lists were downloaded & installed.

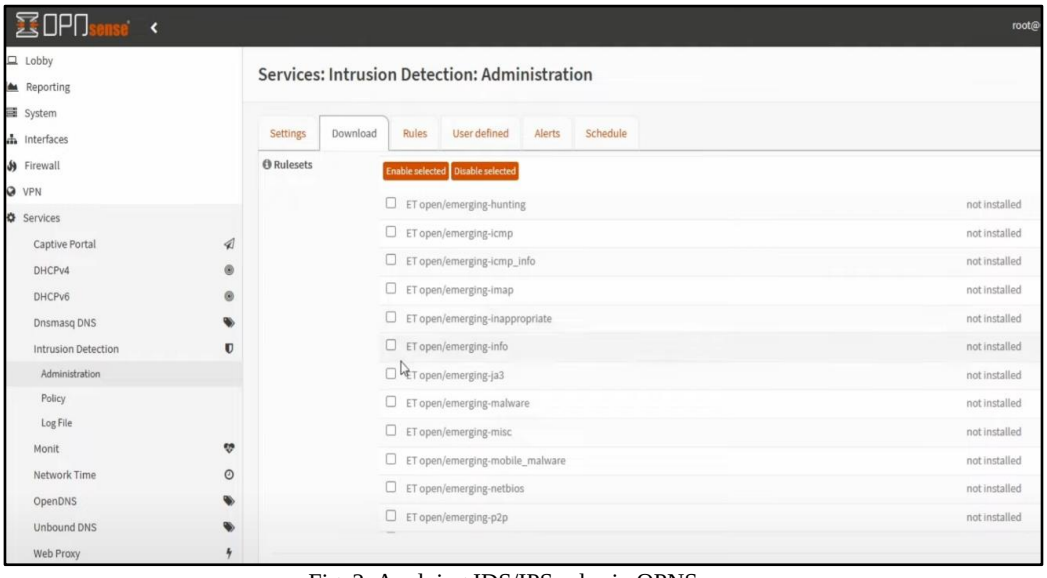

Fig. 2. Applying IDS/IPS rules in OPNSense
Source: author's testing

Additionally, a setup and procedure were created for keeping the servers up to date with the latest FreeBSD & Linux security patches, while minimizing downtime. This included the setup of a high-availability server cluster that would be load-balanced by the open-source solution Traefik (fig. 3). The result of such a setup would be the possibility of patching servers one by one without creating overall downtime for the water utility's network services.

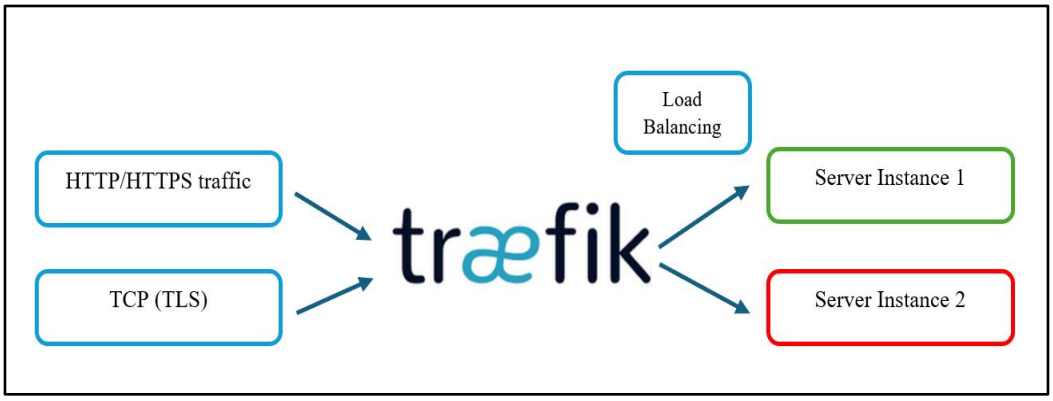

Fig. 3. Traefik load balancer architecture
Source: author's architecture

3. Results

Using Kali Linux on a mobile device in physical proximity to the simulated utility company's HQ, it was possible to scan for the access point SSID, identify it by signal strength and force-disconnect potential target devices that had been connected to it (fig.4).

Fig. 4. Identifying the SSID in Fluxion
Source: author's testing

While scanning for reconnect attempts, a connection hash was then obtained from one of these devices using the Fluxion software, which was afterwards used to compare to the inputted WPA password via the Aircrack-NG method (fig.5).

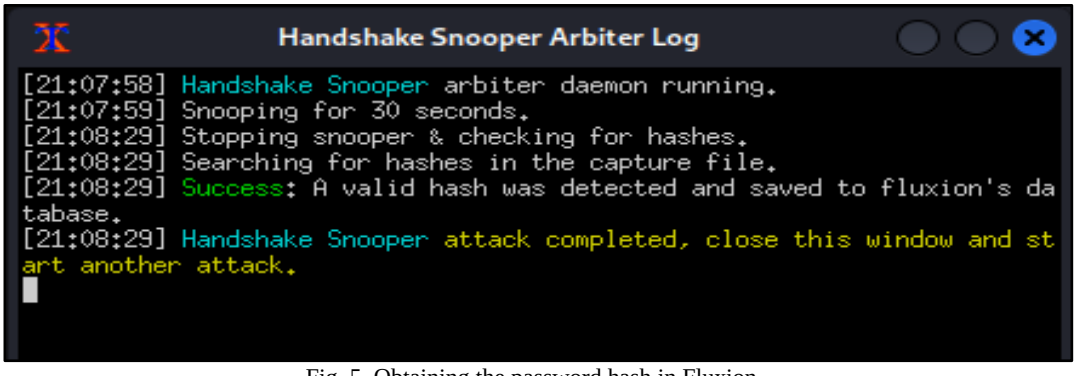

Fig. 5. Obtaining the password hash in Fluxion
Source: author's testing

Aircrack-NG was used to disconnect multiple devices via signal jamming, then spoof the SSID with the expectation that at least one person would succumb to social engineering. This was done by creating a new pop-up in which for them to input their WPA2 key (Fig.

6), which would appear on their device when trying to reconnect to the now malicious network.

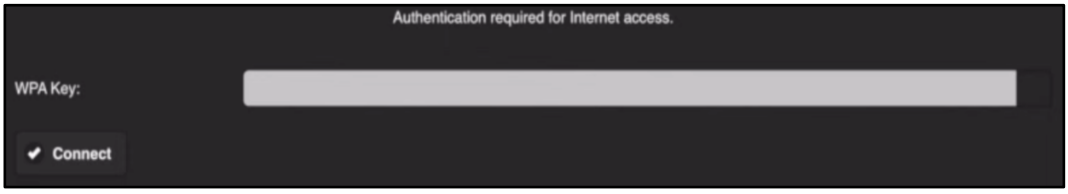

Fig. 6. Malicious popup created by Aircrack-NG for WPA password input
Source: author's testing

A user did input the WPA2 password there for our simulation's purposes, but even if it would not have worked, the hash obtained with Fluxion could be used offline for a brute-force password search until a match would be made, after which the resulting password could be used to connect to the network.

This result revealed the need for MAC address filtering, which was implemented on the network. However, Fluxion can also reveal the MAC addresses of nearby devices, so this only created another step which needed to be done in order to enter the network, i.e. MAC address spoofing for the malicious device. Once a correct MAC address was identified, the device was still able to access the network by spoofing the address.

Once able to access the network, the malicious device could browse across any part of it as a legitimate employee, including the IP address ranges reserved for the servers. VLAN creation in OPNSense managed to restrict this, segregating employee access from the critical network infrastructure (fig.7).

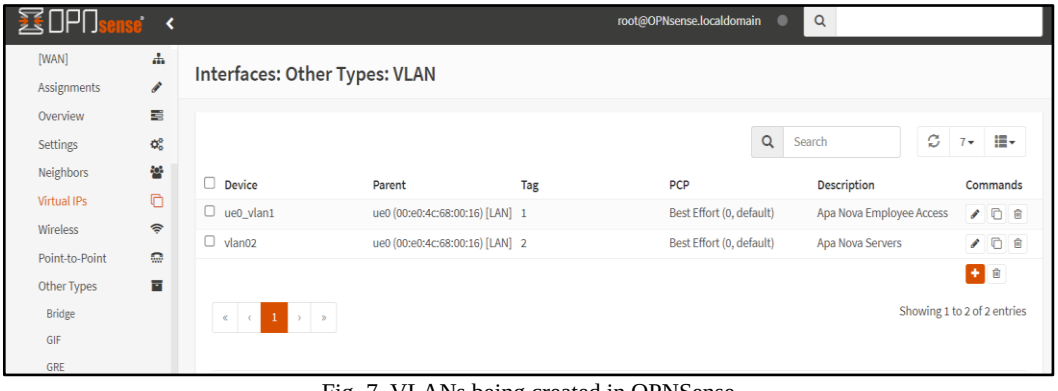

Fig. 7. VLANs being created in OPNSense
Source: author's testing

However, once inside the network, the malicious device was still able to use the packet-sniffing tool Wireshark to obtain access to the unencrypted data that was being transmitted from other users of the network. After making VPN usage mandatory for all remote users of the network, this issue was also mitigated, as connecting via Wi-Fi without also having a Wireguard VPN configuration file was no longer possible (fig.8).

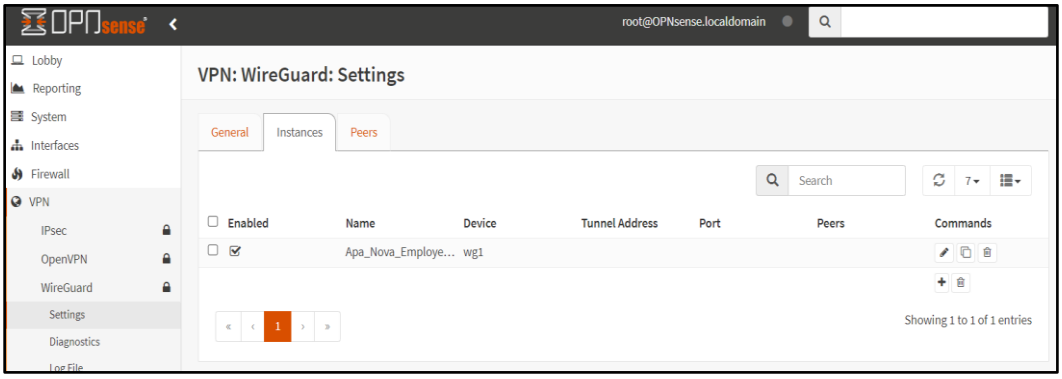

Fig. 8. Wireguard VPN setup in OPNSense
Source: author's testing

Moving on to the results of the shift to the high-availability server solution, over a 30-day period the improvement in downtime from going from the non-redundant server (Non-HA in Fig. 9) to the high-availability cluster (HA in Fig. 9) meant having just 3 downtime events instead of 11, cumulating 46 non-operational minutes instead of 102.

Moreover, the non-operational minutes were solely due to unforeseen technical incidents, not planned outages.

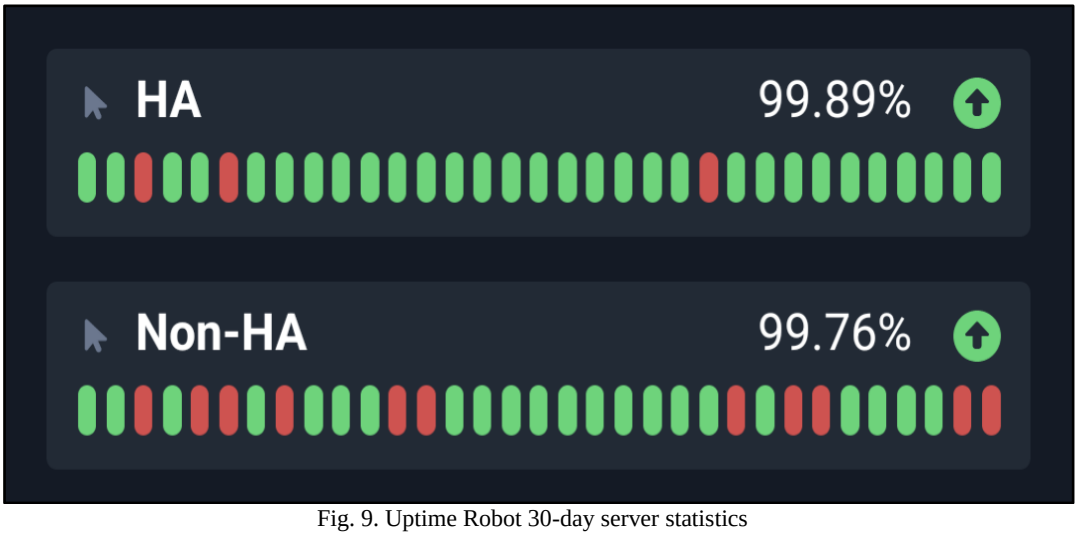

Fig. 9. Uptime Robot 30-day server statistics
Source: author's testing

4. Discussions

4.1. Applicability

The lessons learned during this case study can be applied to any utility or general computing networks that require increased security, decreased downtime & better monitoring of the implemented solutions.

The open-source nature of nearly all software involved also significantly lowers the Total Cost of Ownership and allows for more investment to be made in hardware (such as in adding redundant servers in a cluster) [5].

It should, however, be added that the implementation of any such solution without a constant process of maintenance in order to keep up to date with the latest types of threats would decrease its effectiveness with each passing day.

4.2. Limitations of case study

This case study was performed with real-world hardware & software, but in a simulated situation which only took into account the declared minimum compliance requirements as set forth by the EPA's America's Water Infrastructure Act (AWIA) guidelines [6] and Apa Nova's self-declared 2022 Sustainability Report [7].

While it is possible that water utility companies have higher level of protection or mitigations in place, even as of 2024 the EPA found that 70% of utilities in the USA inspected by federal officials over the past year violated standards meant to prevent breaches or other intrusions [8], being particularly vulnerable to state-sponsored cyberattacks.

Mentioned breaches include basic measures such as changing default passwords or cutting off system access to former employees, so protective measures as described in the case study still seem far from being the norm within these entities.

5. Conclusions

Given that the possible impact of cyberattacks may not just be limited to water service interruptions, but also alter the chemical balances in water treatment plants to dangerous levels, as was the case in Florida in 2021 [9], it is highly important that computer network access control in water utility companies is both properly implemented to begin with and monitored constantly.

It has been proven in the past that even a briefly unpatched server or an account left active can be used as an attack vector, so having a proper policy in place is crucial. Open-source software is a valid solution for lowering the costs and ease of implementation of such a policy and can also be used for post-incident mitigation [10].

It should also be mentioned that when using DPI for identifying potentially dangerous network traffic, recent encryption advances have made this task more difficult. However, it is possible to use AI/ML in order to better understand patterns that create risk within the network [11].

Not covered by this case study were even further steps that should be pursued, such as using dedicated 2-factor authentication keys for employees, which have practically eliminated the risk of phishing at large corporations such as Google [12].

Overall, though, even if not all the described measures are implemented by a water (or other) utility company, every additional layer has been proven to enhance security and improve IT governance and should be pursued if possible.

References

[1] He-Jun Lu și Yang Yu, „Research on WiFi Penetration Testing with Kali Linux," *Complexity*, vol. 2021, 2021.

[2] Niccolo Cascarano, Luigi Ciminiera și Fulvio Risso, „Optimizing Deep Packet Inspection for High-Speed Traffic Analysis," *Journal of Network and Systems Management*, pp. 7-31, 2011.

[3] Ying-Dar Lin, Po-Ching Lin, Viktor K. Prasanna, H. Jonathan Chao și John W. Lockwood, „Deep Packet Inspection: Algorithms, Hardware, and Applications," *IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS*, vol. 32, nr. 10, pp. 1781-1783, 2014.

[4] Charlie King, „Cyber Security in the Power and Utilities Space," 2024. [Interactiv]. Available: https://cybermagazine.com/articles/cyber-security-in-the-power-and-utilities-space.

[5] Joshua M. Pearce, „Economic savings for scientific free and open source technology: A review," *Hardware X*, vol. 8, 2020.

[6] „America's Water Infrastructure Act," 2018. [Interactiv]. Available: https://www.epa.gov/ground-water-and-drinking-water/americas-water-infrastructure-act-2018-awia.

[7] „Raport de sustenabilitate Apa Nova Bucuresti," 2022. [Interactiv]. Available: https://www.apanovabucuresti.ro/assets/pdf/Raport-de-Sustenabilitate-2022-ANB.pdf.

[8] Associated Press, „Cyberattacks on water systems are increasing, EPA warns, urging utilities to take immediate action," 2024. [Interactiv]. Available: https://www.cbsnews.com/news/cyberattacks-on-water-systems-epa-utilities-take-action/.

[9] Jeff Pegues, „Feds tracking down hacker who tried to poison Florida town's water supply," 2021. [Interactiv]. Available: https://www.cbsnews.com/news/florida-water-hack-oldsmar-treatment-plant/.

[10] Tobias Roeder, „TLS 1.3, ESNI, ECH and QUIC: Taming new age cryptography with DPI and AI/ML-based encrypted traffic intelligence," 2023. [Interactiv]. Available: https://www.ipoque.com/blog/cryptography-with-dpi-and-eti.

[11] Ioan Florin Voicu și Daniel Constantin Diaconu, „Monitoring city water incidents via an Internet of Things-based sensor network," *Smart Cities International Conference (SCIC) Proceedings, Smart-EDU Hub*, vol. 10, pp. 207-214, 2022.

[12] Brian Krebs, „Google: Security Keys Neutralized Employee Phishing," 2018. [Interactiv]. Available: https://krebsonsecurity.com/2018/07/google-security-keys-neutralized-employee-phishing/.