yubico

Naftogaz enhances critical infrastructure protection with YubiKeys

Defending Ukraine's national oil and gas company against cyber attacks

Case Study

NAFTOGAZ GROUP

Industry
- Energy
- Public Sector

Benefits
- Passwordless authentication
- Enhanced MFA for privileged users
- Improved user experience

Protocols
- FIDO2

Products
- YubiKey 5 NFC
- YubiKey 5C NFC

Deployment info
- Privileged access
- Remote workplaces

Naftogaz, owned by the Ukrainian state, is a group of companies focusing on oil and gas production. They also specialize in the development of low-carbon energy alternatives, including the construction of waste-processing plants. The biogas produced by Naftogaz is an important part of Ukraine's strategy for developing energy independence and security.

Energy companies play an essential role in the functioning of society, which makes them prime targets for bad actors and rogue states who seek to observe, harm or destroy critical infrastructure. Like major energy companies across the world, Naftogaz isn't only facing physical threats—it is also under attack by cybercriminals. Back in 2020, the then-CEO Andriy Kobolyev revealed that Naftogaz faced around 800 cyber attacks each day.

The responsibility for protecting the organization against these attacks falls to the cyber-security center of Naftogaz-Bezreka, a subsidiary company which provides security for the entire group. Since 2019, the Head of Security Controls for this department has been Oleksandr Tarasov. He manages the testing and implementation of new solutions and platforms within the cybersecurity team and recommends cybersecurity measures to other departments within the Naftogaz group.

Wartime brings unprecedented challenges

As a state-owned institution, Naftogaz has been severely impacted by the Russian war against Ukraine. Oil and gas production around the Black Sea, previously operated by Naftogaz subsidiary Chornomornaftogaz, was disrupted when Crimea was illegally seized in 2014.

Since the major escalation of Russian aggression against Ukraine that began in February 2022, state infrastructure has been under constant bombardment. In December 2022, Naftogaz CEO Oleksiy Chernyshov announced that recent attacks had damaged 350 natural gas facilities operated by the group, with a loss of production valued at $700 million—these losses damage the supply of heating gas for Ukrainians living in the east of the country, endangering lives.

Oleksandr Tarasov,
Head of Security Controls
at Security Operation Center
Naftogaz-Bezreka

> "We can only guess why they are launching attacks, but I think there is probably an aim behind every attack. And the main aim of hackers is data encryption, data theft and to cause panic among the Ukrainian population by destabilizing the energy system."

Physical attacks have been accompanied by cyberwarfare. Petya and NotPetya were large scale ransomware attacks, first identified in 2016, which have been attributed to the Russian state. A major attack in 2017, which predominantly targeted companies operating in Ukraine, caused a reported $10 billion in damages and was described by US government officials as the "most devastating cyber attack in history".

+3500%

increase of cyber attacks in the first month of the war

Defending against cyberwarfare

The escalation of war since February 2022 brought a further increase of cyber attacks. In the first month of the war, cyber attacks on organizations like Naftogaz rose by over 3500%. “From the beginning of the full-scale invasion, we have worked 24/7,” says Tarasov. “It was difficult at first and there were a lot of attacks, which began even before February 24th. There were many attacks on the public sector including on Ukrainian government websites. The first two months were the hardest, but then we began to get used to it.”

Attacks can take many forms. “We can only guess why they are launching attacks, but I think there is probably an aim behind every attack. And the main aim of hackers is data encryption, data theft and to cause panic among the Ukrainian population by destabilizing the energy system,” says Tarasov. As an energy provider, the cybersecurity challenges faced by Naftogaz are complex. While unauthorized access to the operational technology networks could be devastating, some attacks are less threatening. Tarasov explains: “We have a technological network and an IT network so, for example, the Petya attacks had almost no impact on our company. Only the corporate networks suffered the effects.”

Passwords are vulnerable to phishing attacks

Despite operating in unique circumstances, Tarasov experiences similar challenges to cyber security professionals in industries around the world.

“One of the greatest cybersecurity threats is the human factor, through phishing attacks when cybercriminals obtain passwords or credentials,” says Tarasov.

Educating employees was found to have limitations: “We train employees on cyber hygiene and on preventing phishing attacks. It can make a difference, but no matter how much you tell them, everyone can have a weakness. If a hacker comes up with an interesting enough topic for a phishing message, a victim could fall for it.”

Tarasov’s team had a clear goal: to prevent all password leaks. Seeing how phishing could succeed even with well-trained employees, a change of approach was required. “There was an unequivocal decision to introduce security keys and completely get rid of passwords so that users didn’t even have the option to enter them. Until 100% of users have security keys, we won’t be immune to phishing attacks,” says Tarasov.

> “One of the greatest cybersecurity threats is the human factor, through phishing attacks when cybercriminals obtain passwords or credentials.”
>
> Oleksandr Tarasov, Head of Security Controls at Security Operation Center Naftogaz-Bezreka

Security keys offered a more secure alternative to passwords

In 2021, Tarasov attended a Hackathon conference where he met Oleg Naumenko, CEO of Hideez, who explained how—by using FIDO and FIDO2 authentication standards—security keys could offer a user-friendly passwordless experience that could drastically improve an organization's cybersecurity. After the full-scale invasion, Oleg called Tarasov to let him know about Yubico's Secure it Forward program, which offers free YubiKeys for at-risk individuals and organizations involved in the protection of democracy, freedom of speech and human rights. Recognizing the importance of Ukraine's defense against the illegal invasion, and the vital role played by cybersecurity professionals, Yubico donated a total of 20,000 YubiKeys to dozens of Ukrainian governmental agencies and companies who protect critical infrastructure, as well as offering technical assistance to ensure successful implementation.

Tarasov had previously been supportive of using YubiKeys at Naftogaz, but as a governmental agency the purchasing process had been slow and bureaucratic. Receiving YubiKeys as a donation through the Secure it Forward program meant that acquisition could be accelerated. A working group with IT partners was created to expedite implementation, and to solve any issues that arose during deployment. Switching to security keys to protect cloud services was simple, but configuring the new authentication for the on-premise network proved more complex. In total, implementation took around two months.

YubiKeys allow for secure authentication in diverse settings

Naftogaz chose to receive a mixture of YubiKey 5 NFCs and YubiKey 5C NFCs, in order to give employees a choice of authentication using USB-A, USB-C or NFC connections. The keys are used to secure authentication for logging into Windows, workstations and other applications like Microsoft Office 365. The YubiKeys offer enhanced protection for users who require privileged access, as well as enabling safe login for remote workplaces. Not all employees use the YubiKeys for the same purpose, says Tarasov: "Some only use the keys to enter their workstation or to enable remote access, while other groups use the keys to access up to seven different services."

Users enjoy the convenience of YubiKeys. "The first thing users think about is that they don't have to enter a password. They just connect the YubiKey, type in four or six digits, and continue working. There is no need to get your phone and check it. If users need to lock their device, they just pull out the key and go about their business," says Tarasov. He admits that, predictably, new technology is more quickly embraced by younger employees: "The younger workers love the keys. They are interested in new gadgets and see YubiKeys as innovative. It's definitely a bit harder for the older generation, but we are getting there step by step."

> "Users no longer have to enter a password. They just connect the YubiKey, type in four or six digits, and continue working. There is no need to get your phone and check it."
>
> Oleksandr Tarasov, Head of Security Controls at Security Operation Center Naftogaz-Bezreka

Moving toward passwordless authentication for all employees

At Naftogaz, YubiKeys are currently only used within Naftogaz-Bezreka, the subsidiary focused on security. Tarasov is pleased with the results so far: “I think you can already see the extremely low probability of phishing attacks within Naftogaz-Bezreka. It is through using YubiKeys and Microsoft Azure, where we link our keys, that users no longer need to use passwords. In my opinion, Naftogaz-Bezreka is the most secure company in our group.”

Tarasov has ambitious plans for the future: “The next step is for YubiKeys to cover the entire infrastructure of the company and to set up passwordless authentication for VPN connections and the entire network in general. We are currently planning to implement YubiKeys in another company, also part of the Naftogaz group. As the company is scattered across Ukraine, we need to work with many different IT units. They are busy with their own work, but it is important to get it done. Our vision is that we must get rid of passwords—that means no passwords at all.”

Tarasov is convinced that passwordless authentication is the future for secure authentication: “I think passwords are a thing of the past. We need to look to the future and move with the times. The YubiKey could be compared to the latest iPhone or a Tesla. Passwords are more like using a push-button telephone or driving an old Soviet car. You need to keep moving forward, striving for excellence and innovation—this way users and administrators alike will be happy.”

> “You can already see the extremely low probability of phishing attacks within Naftogaz-Bezreka. It is through using YubiKeys and Microsoft Azure, where we link our keys, that users no longer need to use passwords. In my opinion, we are the most secure company in our group.”
>
> Oleksandr Tarasov, Head of Security Controls at Security Operation Center Naftogaz-Bezreka

Learn more yubi.co/customers | yubi.co/energy

About Yubico As the inventor of the YubiKey, Yubico makes secure login easy. As a leader in setting global standards for secure access to computers, mobile devices, and more, Yubico is also a creator and core contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor (U2F), and open authentication standards. For more information, please visit: www.yubico.com.