sosafe

DEW21

CUSTOMER STORY

DEW21

Dortmunder Energie- Und Wasserversorgung GmbH

A pioneer in cyber security awareness
for critical infrastructures in Europe

The Company

DEW21

DEW21 is a local energy supplier in Dortmund with around 1,000 employees operating in the regulated energy sector and is ISO 27001 certified in accordance with the Energy Industry Act. They supply electricity, gas, water, and heat to around 600,000 people in and around Dortmund.

Industry	Employees	Revenue
Energy (Utility)	> 1,000	1,200 Mio € (2022)

The Challenge

Strengthening human risk management by fulfilling the requirements from regulations like NIS2

As one of the larger operators of critical infrastructure in Dortmund, DEW21 was looking for a security awareness solution that could then be transferred smoothly to the other organizations in the 21 Group and would help with the upcoming European regulations like NIS2, while helping them manage human risk better.

> "In the midst of the regulated critical infrastructure sector, we face significant challenges, from implementing the NIS2 Implementation Act to adapting to the EU CER regulation. Together with the other infrastructure companies in the 21 Group in Dortmund, we were looking for solutions to overcome these challenges and build a robust online future in this regulated sector that we are in."

Jens Feistel
CISO DEW21

The Solution

Ready-to-use awareness training that adapts to changing needs, supports compliance, and encourages secure behaviors

SoSafe's awareness training helps to meet NIS2 requirements for awareness training and risk analysis, and SoSafe's best-practice recommendations can easily be extended to the rest of the group.

"Cyber security needs to be addressed in small, manageable doses on an ongoing basis. Regular phishing training, combined with the short e-learning sessions, does just that. And employees are now realizing that this is to their benefit because what they have learned is also helpful in their personal lives."

Jens Feistel
CISO DEW21

Increasing awareness through multichannel solutions:

- E-learning and phishing simulations with little effort according to SoSafe recommendations
- Use of the phishing report button and feedback from their IT service provider
- Introduction of Sofie Rapid Awareness

The Results

Paving the road for regulatory compliance while sustainably improving user resilience

Click rates of the phishing simulation were already significantly reduced in the first year and acceptance of the entire awareness campaign increased enormously after some initial skepticism.

"We now have well-sensitized employees who recognize suspicious emails early on and then proactively approach the email senders and individually reach out to them: 'Hey, you might have a problem.'"

Jens Feistel
CISO DEW21

That's why DEW21 recommends SoSafe:

- Click rate decreased by 54 % in the first year
- Successful detection and reporting of the phishing simulation in 43 % of cases
- 4.9/5 rating by employees

> In a crisis, no technology will help you – only resilient colleagues who keep a cool head even in such a stressful situation, apply what they have learned, and do their best to get the company back on track. SoSafe is the solution provider that helps us to get there quickly and to engage our employees in an appealing way.

Jens Feistel
CISO DEW21

Prepare for NIS2 and other regulations with SoSafe.

Explore our solutions →

Interview with Jens Feistel, CISO at DEW21

DEW21 successfully implemented phishing and e-learning best practices and acts as a pioneer to serve as a role model for other organizations in Dortmund's infrastructure. Employees are made aware of the training courses through regular reminders on various channels. In addition, the phishing report button was introduced, where an IT service provider checks the incoming reports and provides feedback. The future integration of Sofie Rapid Awareness will further strengthen the organization's security measures.

What is the cooperation with other infrastructure organizations in Dortmund like?

In Dortmund, we have a large network of different services from the municipal environment. I have succeeded in building up a network of interested parties in the municipal environment (administration, public transport, waste disposal, telecommunications, water) in order to do something together for IT security and security awareness. Because no matter which of us is hacked, everyone is affected. That is why we have joined forces to find a solution together. In SoSafe, we have found a reliable partner to initially set up a phishing campaign together. By joining forces, we were not only able to achieve attractive conditions, but also standardization for all parts of the 21 Group. This meant that each company did not have to think independently about how the campaign should be planned and rolled out, but we were able to set a standard and the other companies followed suit.

How has the internal acceptance of the training developed for you?

In the beginning, many employees wondered why they had to do this now. But that changed over time. One reason for this was the targeted approach. You can't avoid addressing the various people directly, appointing a clear internal contact person and approaching the individual departments. But the situation outside the company also helped colleagues to understand. It's not just a burden and it's not just to do with business, it just helps me in my private life, too.

You recently added Sofie – Rapid Awareness, our Microsoft Teams integration – what do you expect from using Sofie?

I expect Sofie to simply send the information directly to our employees' cell phones and to immediately alert them to the message via push. When they are on their way back from the construction site to the office or back to work, the employees take a look and realize, 'Oh, there's a message that concerns and affects me in some way.' We are aware that people pause a little longer and read through the news. The majority of employees in the company understand the importance of digitalization issues in general and the associated awareness of everything that now surrounds us – from smartphones to private streaming services in the evenings.

What would you recommend to other organizations in the public sector/critical infrastructure in terms of cyber security awareness?

Just start, just try it out. The crucial point is to get started, set sail, see which way the wind is blowing and readjust the sails if necessary. The aim must be to create a more resilient company, and I believe that this can be achieved by investing in employees and their training. We have to learn to adapt to new things and adjust as technologies evolve. That's the big challenge.