

CUSTOMER STORY

# DEW21

Dortmunder Energie- Und  
Wasserversorgung GmbH

Ein Vorreiter für Cyber Security Awareness im  
regulierten Sektor in Dortmund - und deutschlandweit



## Das Unternehmen

DEW21

## Die Herausforderung

Erfüllung der Anforderungen von Vorschriften wie NIS2 in einer effektiven Trainingsmaßnahme

Als lokaler Energieversorger in Dortmund mit rund 1.000 Mitarbeitenden im regulierten Bereich der Energiewirtschaft tätig und gemäß dem Energiewirtschaftsgesetz nach ISO 27001 zertifiziert, versorgt die DEW21 rund 600.000 Personen in und um Dortmund mit Strom, Gas, Wasser und Wärme.

Industrie	Anzahl der Mitarbeitenden	Umsatz
Energieversorgung	> 1.000	1.200 Mio. € (2022)

Als einer der größeren Betreiber Kritischer Infrastrukturen in Dortmund war DEW21 auf der Suche nach einer Security-Awareness-Lösung, die problemlos auf die anderen Organisationen der 21-Gruppe übertragen werden kann und die bei der Umsetzung der anstehenden europäischen Vorschriften wie NIS2 unterstützt.

„Inmitten des regulierten Sektors kritischer Infrastrukturen stehen wir vor Herausforderungen wie der Anpassung an das NIS2-Umsetzungsgesetz oder die EU-CER-Verordnung. Gemeinsam mit den anderen Infrastrukturunternehmen der 21-Unternehmensgruppe in Dortmund haben wir nach Lösungen gesucht, um diese Herausforderungen zu bewältigen und eine robuste Zukunft im regulierten Sektor aufzubauen.“



**Jens Feistel**  
CISO DEW21

## Die Lösung

Sofort einsetzbare Awareness-Trainings, die sich an veränderte Anforderungen anpassen lassen und die die Einhaltung von Compliance-Richtlinien unterstützen

## Die Ergebnisse

Den Weg für die Einhaltung von Vorschriften ebnen und gleichzeitig die Resilienz der Nutzenden nachhaltig verbessern

Die Awareness-Schulung von SoSafe unterstützt die Einhaltung der NIS2 Anforderungen für Schulungen und Analysen, und die Best-Practice-Empfehlungen können leicht auf die ganze 21-Unternehmensgruppe ausgeweitet werden.

„Cyber Security muss kontinuierlich in kleinen, verträglichen Dosen adressiert werden. Die regelmäßige Phishing-Maßnahme, kombiniert mit den kurzen E-Learnings, erfüllt genau diesen Zweck. Und mittlerweile erkennen die Mitarbeitenden, dass das zu ihrem Vorteil ist, weil das Erlernete auch im Privatbereich hilfreich ist.“



**Jens Feistel**  
CISO DEW21

### Steigern der Awareness durch die Multichannel-Lösungen:

- E-Learning und Phishing-Simulation mit wenig Aufwand gemäß SoSafe Empfehlungen
- Nutzung des Phishing-Meldebuttons und Feedback durch den IT-Service Provider
- Einführung von Sofie Rapid Awareness

Bereits im ersten Jahr konnten Klickraten der Phishing-Simulation signifikant gesenkt werden und die Akzeptanz der gesamten Maßnahme wurde nach anfänglicher Skepsis enorm erhöht.

Wir haben inzwischen viele gut sensibilisierte Mitarbeitende, die verdächtige E-Mails frühzeitig erkennen und dann proaktiv auf E-Mail-Absender zugehen und sie gezielt ansprechen: „Ich glaube ihr habt da ein Problem.“



**Jens Feistel**  
CISO DEW21

### Deshalb empfiehlt die DEW21 SoSafe weiter:

- Senkung der Klickrate um 54 % im ersten Jahr
- Erfolgreiches Erkennen und Melden der Phishing-Simulation in 43 % der Fälle
- 4.9/5 Bewertung durch die Mitarbeitenden



Im Krisenfall hilft dir keine Technik, da helfen dir nur resiliente Kolleginnen und Kollegen, die eben auch in so einer Stresssituation einen kühlen Kopf bewahren, das Erlernte anwenden und ihr Bestes geben, um das Unternehmen wieder auf Kurs zu bringen. SoSafe ist der Anbieter, der uns dabei hilft, schnell ans Ziel zu kommen und unsere Mitarbeitenden auf ansprechende Art und Weise einzubinden.



**Jens Feistel**  
CISO DEW21

**Bereiten Sie sich mit SoSafe auf NIS2 und andere Vorschriften vor.**

Produktdemo vereinbaren →

## Interview mit Jens Feistel, CISO DEW21



DEW21 hat erfolgreich Phishing- und E-Learning-Best Practices implementiert und fungiert als Vorreiter, um anderen Organisationen in der Dortmunder Infrastruktur als Vorbild zu dienen. Mit regelmäßigen Erinnerungen auf verschiedenen Kanälen werden die Mitarbeitenden auf die Schulungen hingewiesen. Zudem wurde der Phishing-Meldebutton eingeführt, wobei ein IT-Serviceprovider die eingehenden Meldungen überprüft und Feedback gibt. Die zukünftige Integration von Sofie Rapid Awareness verstärkt zusätzlich die Sicherheitsmaßnahmen der Organisation.

### Wie sieht die Zusammenarbeit mit den anderen Organisationen der Infrastruktur in Dortmund aus?

In Dortmund haben wir ein großes Geflecht an verschiedenen Dienstleistungen aus dem kommunalen Umfeld. Mir ist es gelungen, ein Netzwerk von Interessierten im kommunalen Umfeld (Verwaltung, ÖPNV, Entsorgung, Telekommunikation, Wasser) aufzubauen, um gemeinsam etwas für die IT-Sicherheit und Security Awareness zu tun. Denn egal, wer von uns gehackt wird, alle sind davon betroffen. Daher haben wir uns zusammengeschlossen, um gemeinsam eine Lösung zu finden. Mit SoSafe haben wir einen zuverlässigen Partner gefunden, um gemeinsam zunächst eine Phishing-Kampagne durchzuführen. Durch den Zusammenschluss konnten wir nicht nur attraktive Konditionen, sondern auch eine Standardisierung für alle Teile der 21-Unternehmensgruppe erwirken. So musste sich nicht jedes Unternehmen eigenständig überlegen, wie die Kampagne geplant und umgesetzt werden soll, sondern wir konnten einen Standard setzen und die restlichen Unternehmen folgten diesem.

## Wie hat sich die interne Akzeptanz des Trainings bei der Belegschaft entwickelt?

Am Anfang fragten sich viele Mitarbeitende, warum sie das jetzt machen müssen. Aber mit der Zeit hat sich das geändert. Gründe dafür waren einerseits die zielgruppengerechte Ausrichtung. Man kommt nicht umhin, die verschiedenen Personen direkt anzusprechen, einen klaren internen Ansprechpartner zu benennen und auf die einzelnen Fachbereiche zuzugehen. Aber auch die Situation außerhalb des Unternehmens hat dazu beigetragen, dass die Kolleginnen und Kollegen verstanden haben: Das ist nicht nur Last und hat nicht nur mit dem Geschäft zu tun, sondern es hilft mir eben auch in meinem privaten Umfeld weiter.

## Ihr habt kürzlich Sofie Rapid Awareness, unsere Microsoft Teams-Integration, hinzugefügt – was erwarten Sie von der Nutzung von Sofie?

Ich erwarte von Sofie, dass die Informationen einfach direkt auf die Handys unserer Mitarbeitenden kommen und sie per Push auch umgehend auf die Nachricht aufmerksam gemacht werden. Wenn sie auf dem Rückweg von der Baustelle ins Büro oder zurück in den Betrieb sind, schauen die Mitarbeitenden mal drauf und stellen fest „oh da ist eine Nachricht, die mich in irgendeiner Art und Weise anspricht und tangiert.“ Bei uns ist das Bewusstsein vorhanden, dass man etwas länger innehält und sich Nachrichten durchliest. Ein Großteil der Mitarbeitenden im Unternehmen versteht, wie wichtig Themen rund um die Digitalisierung im Allgemeinen und die damit einhergehende Sensibilisierung für alles ist, was uns mittlerweile umgibt – angefangen vom Smartphone bis zum privaten Streamingdienst in den Abendstunden.

## Was empfehlen Sie anderen Organisationen im öffentlichen Sektor/in den kritischen Infrastrukturen in Bezug auf Cyber Security Awareness?

Einfach anfangen, einfach ausprobieren. Der entscheidende Punkt ist: Loslegen, die Segel setzen, schauen aus welcher Richtung der Wind weht und gegebenenfalls die Segel nachjustieren. Das Ziel muss doch sein, ein resilienteres Unternehmen zu schaffen, und dieses erreicht man meiner Meinung nach, wenn man in die Mitarbeitenden und in ihr Training investiert. Wir müssen lernen, uns auf neue Dinge einzustellen und uns anzupassen, wenn sich die Technologien entwickeln. Das ist die große Herausforderung.