SECFENSE + Sandis

Case Study

Implementation of User Access Security Broker in the WAGAS group

Sandis selected and implemented the Secfense solution in the WAGAS Group to quickly secure 27 different applications and over 5,000 users and to implement the recommendations of the Polish Financial Supervision Authority and implement the requirements of the DORA regulation.

Sandis is an integrator and software supplier for the insurance industry. It offers software for the distribution of insurance products, as well as infrastructure management and application development services. The Sandis application is used every day by thousands of insurance product sellers, and the solutions offered support the handling of many nationwide contacts.

One of the pillars of the company's strategy is to provide recipients with a high standard of security for the data they process. That's why Sandis is paying a lot of attention to new cybersecurity requirements, especially those imposed on the entire industry.

Recommendations of the Polish Financial Supervision Authority and the DORA regulation and strong authentication

On October 19, 2022, the position of the Office of the Polish Financial Supervision Authority on the activities of insurance and reinsurance companies in the field of cybersecurity was published. The Commission Office emphasizes that "in the face of intensified activities of cybercriminals, not using strong, multi-factor customer authentication is an unacceptable risk."

Additionally, on January 16, 2022, the DORA (Digital Operational Resilience Act) regulation entered into force, which is part of the European Union's cybersecurity strategy. Companies and institutions have until January 17, 2025 to adapt to the new regulations. And these regulations, which also cover external ICT service providers to entities operating in the financial industry, require the implementation of policies and protocols for strong authentication mechanisms as part of ICT risk management.

Sandis situation before implementation

Due to these requirements, Sandis, in cooperation with the WAGAS group, faced the challenge of securing both the applications it offers and those of external suppliers. Sandis decided to introduce additional protection in the form of multi-factor authentication mechanisms based on FIDO, so that application users can log in safely, avoiding popular cyber threats - phishing, account takeover and theft of their own and customers' data.

The project was hampered by the multitude of systems, diversity of technologies and age of some applications. As part of the pre-implementation analysis, the company verified that users use very different client platforms: desktop computers, laptops, tablets, smartphones and traditional mobile phones. Each of these devices differs in technological advancement and functions, as well as in the level of security.

Solutions provided to thousands of users in the WAGAS Group are hosted in three data centers. And they are used by many thousands of users:

3
Data Centers

+27
Applications

- **DA 1:** 14 applications
- **DA 2:** 4 applications
- **DA 3:** 9 applications

Main challenges:

- various technologies
- many suppliers
- applications at various stages of the development cycle, currently being developed and maintained, those being phased out and those "retired"
- providing an MFA solution that has a standardized look and feel

Choosing a solution

Sandis took into account two different operating scenarios - the implementation of MFA mechanisms within individual applications and the use of a centralized, unified solution such as Secfense.

Secfense provides the User Access Security Broker solution, which allows you to quickly apply strong authentication to any system and application, without interfering with their code.

Sandis made its choice by analyzing TOC - Total Cost of Ownership, i.e. the full picture of costs **"from purchase to retirement"**. The key elements analyzed include:

- CAPEX – expenditure
- OPEX – maintenance, development
- hidden costs: downtime, loss of productivity, peer support

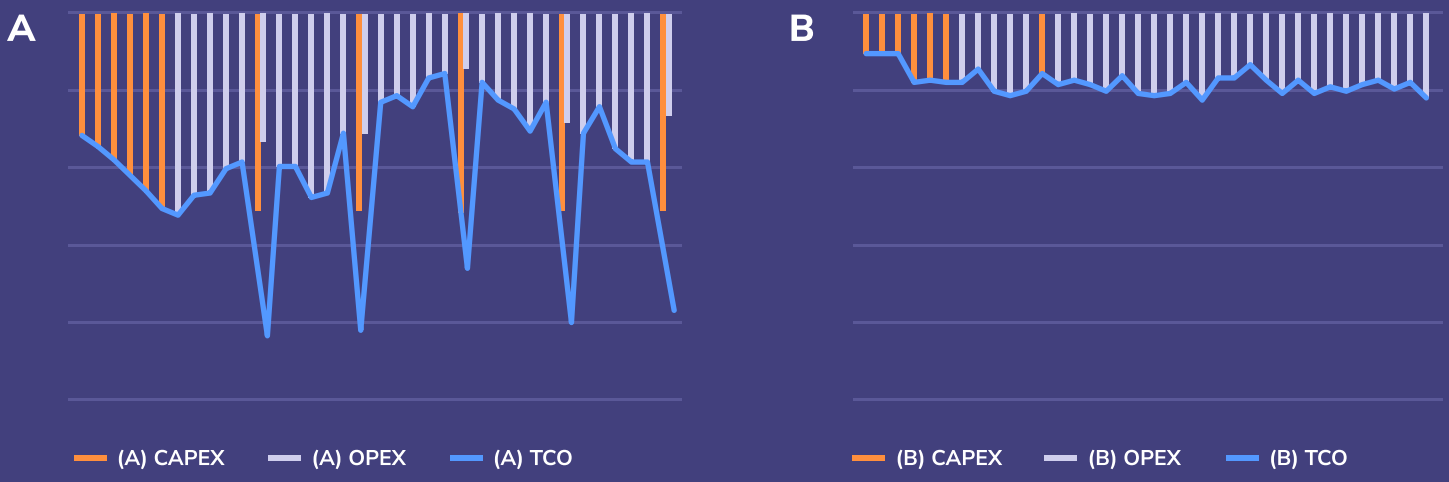
The company took into account, among others:

- initial development
- development in the life cycle
- maintenance
- administration
- costs of lack of consistency (training, call center support, helpdesk support)

A comparison of the costs of both scenarios (scenario A - organic implementation and scenario B - implementation of User Access Security Broker) left no doubts about the greater profitability of using the Secfense solution. Implementing MFA security at the level of each application separately would be too expensive, long-lasting and difficult to maintain.

Scenario analysis

Sandis



Other important features of the Secfense solution

Sandis also noted other features of User Access Security Broker:

- allows you to implement strong authentication mechanisms on many applications in a few weeks
- does not require any modification to the code
- allows any second factor of authentication to be used

In addition to FIDO, a dedicated mobile application and one-time passwords generated by applications such as Authenticator, Sandis also provides the option of authentication using codes available on all client devices sent via SMS or e-mail.

Implementation process

Already in the first stage of implementation, Sandis secured 11 of its applications, and ultimately provided security for 27 applications hosted in three different data centers.

The speed and ease of implementing User Access Security Broker allowed Sandis to skip the Proof of Concept stage. The company's team found that the simple implementation and licensing method based on a subscription containing, among others, support allows you to immediately move to the implementation and production stages.

Effect of implementing User Access Security Broker

Sandis very quickly provided modern protection to over 5,000 users. And today it is fully prepared to secure subsequent applications and ensure compliance with European Union regulations and the recommendations of the Polish Financial Supervision Authority.