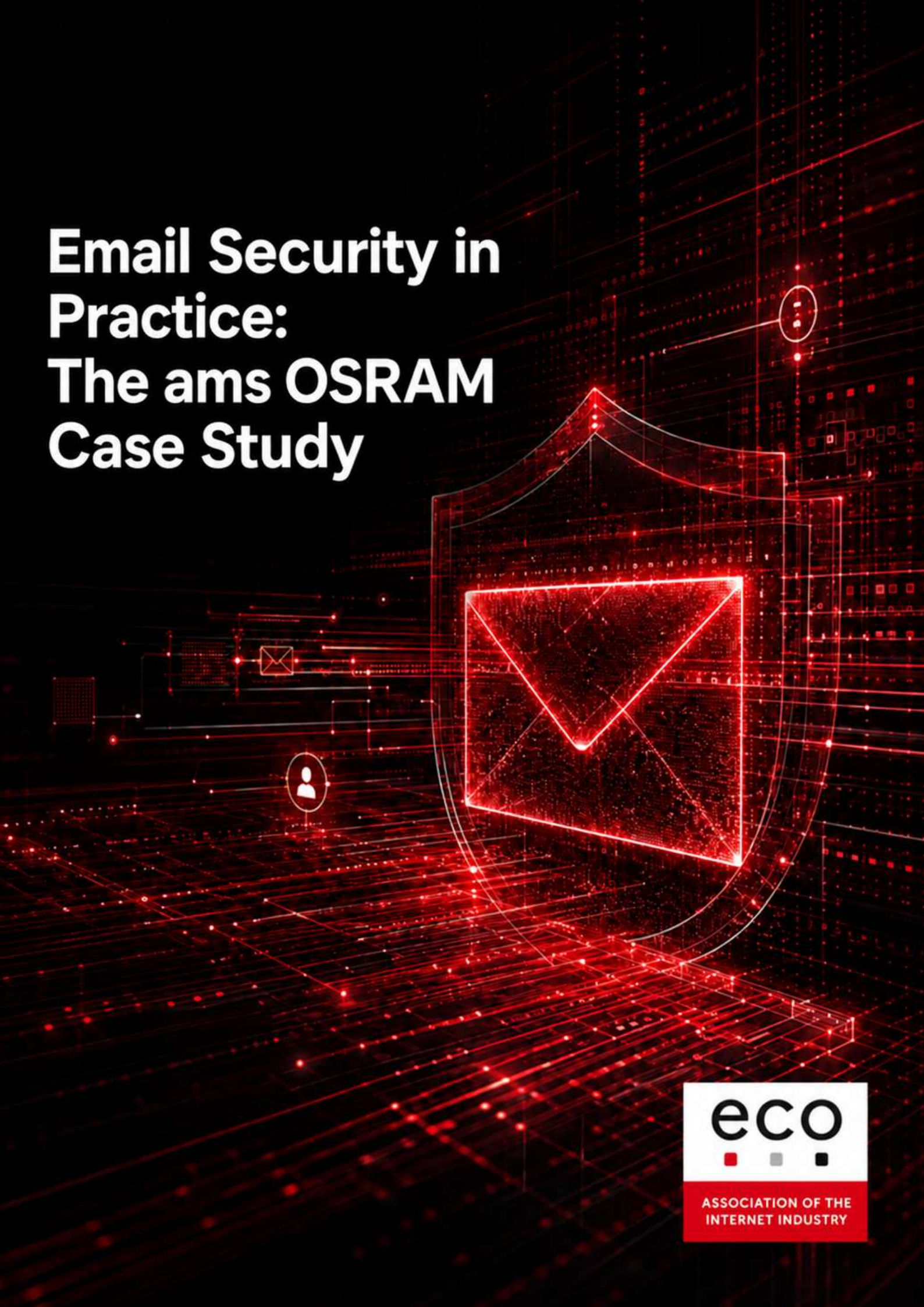
Email Security in Practice: The ams OSRAM Case Study



eco

ASSOCIATION OF THE INTERNET INDUSTRY

Table of contents

Introduction

For decades, email has been the most important means of communication in the business world – and, at the same time, the main gateway for cyberattacks. The latest data from the German Federal Office for Information Security's (BSI) final report on email security illustrates the scale of the threat: around 360 billion emails are sent worldwide every day. Attackers consistently exploit this enormous volume, as over 90 per cent of all cyberattacks begin with a phishing email.

The economic consequences are massive: cybercrime currently causes over EUR 200 billion of damage in Germany every year. Despite these risks, many companies remain inadequately protected: over 30 % of all organisations still do not have a DMARC record in place that would protect against phishing, leaving them vulnerable to identity theft and brand misuse.

Cost-benefit analysis: prevention versus incident response

Aspect	Implementation (prevention)	Cyberattack (consequences of an incident)
Direct costs	One-off configuration time for IT/service providers; certificate costs for DANE (often low).	An average of EUR 2.5 million per incident (including forensics, recovery and ransom).
Operational workflow	Seamless integration in the background; no disruption to day-to-day business.	Downtime: potential loss of communication for days; loss of orders and delivery delays.
Reputation	Enhanced reputation: Partners view your emails as secure and verified (green padlock/tick) and can immediately discard fake emails.	Loss of trust: customers receive phishing emails sent in your name; lasting damage to your brand.
Legal / Compliance	Compliance with NIS2 and GDPR requirements (state of the art).	Fines: Severe penalties if negligence is proven; personal liability risks.

A practical example from ‘ams OSRAM’ shows that SPF, DKIM and DMARC can be successfully implemented with a clear strategy and a step-by-step approach. These measures have been in place since 2017. The study identifies the key success factors and provides practical recommendations on how companies can protect their digital identity and build resilience against modern cyber threats.

Fundamentals of email security

The key technologies that ensure the authenticity and integrity of emails are:

- **SPF (Sender Policy Framework):** Prevents emails with a forged envelope sender from being accepted.
- **DKIM (DomainKeys Identified Mail):** Ensures that emails are accompanied by a cryptographic signature from the sender.
- **DMARC (Domain-based Message Authentication, Reporting and Conformance):** Builds on SPF and DKIM, protects the "From" address visible in the email client and enables policy control (none, quarantine, reject).

When used in combination, these methods provide an effective set of tools for identifying and blocking fraudulent emails. Email is business-critical. For CEOs and decision-makers, email security is therefore no longer merely an operational IT task, but a matter of business continuity and safeguarding trust. Implementing technologies such as DMARC and consistently using authentication standard, are strategic investments.

- **Protecting brand reputation:** DMARC prevents criminals from misusing your domain for fraudulent emails (e.g. CEO fraud), thereby undermining the trust of your customers and partners.
- **Minimising liability:** In light of increasing regulatory requirements (e.g. NIS2), using these technologies demonstrates compliance with best practice and reduces legal risks

Initial situation

Before the project began, the company had limited transparency regarding the actual sources of email messages. Several domains had inadequate or missing SPF, DKIM or DMARC records. In addition, there were regular spoofing attempts, which posed a high risk to customers, partners and internal staff.

The helpdesk received recurring reports of fake emails, and the marketing department reported falling delivery rates for campaigns. At the same time, regulatory requirements were increasing, including BSI recommendations and best practices for enhanced email security. This initial situation called for a structured, low-risk and transparent modernisation project.

Objectives

The project pursued four key objectives:

- **To protect the brand identity** by consistently reducing spoofing attacks.
- **To improve email deliverability,** particularly in communications with customers and partners.
- **Establishing complete transparency** regarding all legitimate and illegitimate sending sources.
- **To ensure regulatory compliance** in line with BSI guidelines and data protection requirements.

These objectives were achieved without any operational disruption to live email traffic.

Process models for companies

Successful implementation is based on a phased approach, comprising three clearly defined phases:

1. Short-term measures (quick wins):

- Enable SPF and DMARC with a ‘hard’ policy for all domains without an MX record. “v=spf1 –all”
- For production domains, initially select ‘soft’ settings to minimise risk. “v=spf1 ~all”
- Initially configure DMARC with the “none” policy and rua=… to collect reports. Implement transport rules to flag suspicious emails. For example, flag all emails where SPF (or DMARC) fails with a label such as 'Potentially faked sender'. This can be done by setting up a transport rule in Exchange, for example.
- Emails from your own domains can be treated more strictly than those from third parties, as they may simply result from configuration errors. Therefore, it is better to use only a warning label rather than a hard rejection.
- Enable DKIM for all domains.
- Send copies of emails that fail SPF for your domains to an analysis mailbox to identify potentially legitimate but unknown senders. Once the analysis is complete, delete such emails.
- Ensure that your SPF string is shorter than 255 characters and involves no more than 10 DNS lookups. Use subdomains if specific settings are required, e.g. hr.<domain.com> for emails from the HR system.
- Validate your settings, for example, by using.
- https://mxtoolbox.com/SuperTool.aspx?action=spf%3a<IhreDomain>https://mxtoolbox.com/SuperTool.aspx?action=spf:<IhreDomain

2. Medium-term measures:

- Evaluate incoming DMARC reports.
- Identify and reconfigure legitimate sending sources (e.g. CRM systems and third-party newsletters).
- Gradually tighten policies (SPF → “-all”, DMARC → “reject”).
- Delete emails that arrive from an unauthorised source and use one of your company domains (once all legitimate servers have been identified).

  This rule will protect you from thousands of spam and phishing emails. For analysis purposes, store a copy of the rejected email in a security review folder at first.

3. Long-term measures:

- Establishment of ongoing monitoring.
- Systematic domain management to minimise attack surfaces.
- Integration of these measures into business continuity strategies and security awareness programmes.

DMARC POLICY: : Technical check of the domain configuration

SPF, DKIM and DMARC working together

Three layers of protection for authentic senders, message integrity and controlled policies

SPF	DKIM	DMARC
Verify the sender	Sign the message	Enforce policy

SPF ⟶ DKIM ⟶ DMARC ⟶ robust domain reputation

SPF · Sender Policy Framework

Benefits

Checks whether the envelope sender is sending from a source (IP address) authorised for the domain

CONFIGURATION

Domains without an MX record: “v=spf1 -all”.

- For production domains, start with “v=spf1 ~all”, then tighten the policy to “-all” following verification.
- Keep the SPF string under 255 chars and a maximum of 10 DNS lookups; use subdomains for special cases.
- Validate the configuration regularly and identify unknown legitimate sending sources via an analysis mailbox.

DKIM · DomainKeys Identified Mail

Benefits	CONFIGURATION
Cryptographically signs emails. Receiving mail servers verify the signature using the key published in the DNS.	Configure at least two selectors per DNS domain that point to the email provider's keys. Example for Microsoft: Selector1._domainkey CNAME selector1-company-com._domainkey.<tenant>.onmicrosoft.com.</tenant> Selector2._domainkey CNAME selector2-company-com._domainkey.<tenant>.onmicrosoft.com.</tenant> Then activate the keys in the email provider's administration portal (for MS: Go to https://admin.exchange.microsoft.com/)

DMARC · Policy, reporting and protecting the From-field

Benefits	CONFIGURATION
Complements SPF and DKIM with policies on how to handle errors and provides insight into legitimate use and abuse.	Enable hard DMARC for all your domains without an MX record to reduce the risk of abuse. _dmarc.<domain>. ==> TXT "v=DMARC1; p=reject;"</domain> Enable soft DMARC for all other domains (change this to "p=reject" later). _dmarc.<domain>. ==> TXT "v=DMARC1; p=none; aspf=r; adkim=r; fo=0; ri=84600; rua=mailto:dmarc@<domain>"</domain></domain> Analyse emails sent to your "dmarc" mailbox, as specified in the rua parameters, to identify applications that send on behalf of others and require specific configurations for DMARC support. Forensic reports (fo=1, ruf=<email>) may lead to legal issues under the GDPR. As these are almost never sent, it is best to disable them (fo=0)</email>

Objective: Detect forgeries, reliably deliver emails from legitimate senders, and tighten policies in a controlled manner.

EXCHANGE RULE: HANDLING UNAUTHORISED SENDERS	SPF HARD FAIL: PRODUCTION RULE CONFIGURATION

Challenges

During the project, the team encountered the following typical challenges:

- Inadequate or completely missing documentation for email sending sources that had developed over time.
- Shadow IT: unexpected newsletter and automated email systems
- Inadequate DKIM support in older systems
- Complicated configuration of some cloud systems, such as Atlassian, for “send-on-behalf” scenarios.
- Dealing with DMARC reports requires consideration of data protection issues (forensic reports can pose problems).
- Conflicting interests between departments (e.g. Marketing vs. Security)

The team successfully overcame these challenges through structured, open communication, a centralised reporting inbox and clearly defined responsibilities.

Business value

Implementing SPF, DKIM and DMARC offers companies clear business benefits:

- Ensuring a high delivery rate to partners and customers.
- Reducing the workload of the helpdesk and support teams caused by fraudulent emails.
- Contributing to regulatory compliance (e.g. BSI recommendations, NIS2, data protection requirements).
- Transparency across all sending systems, including consolidated third-party providers.

- The more companies that participate, the easier it is for recipients to filter out suspicious emails. If everyone set DMARC to “none”, a very high filter rate would be achieved without any risk whatsoever.

These results provide measurable business value and increased the long-term resilience of the communications infrastructure.

Lessons learned

The project yielded several key insights:

- An iterative approach minimises risks and facilitates the tightening of policies.
- Early involvement of management speeds up decision making.
- Centralised technical governance prevents misconfigurations in the long term.
- End users and staff must be made aware of the issues at an early stage so that they understand and accept labelling and warning messages.
- Transparent communication between the IT, security and business departments is essential.

Recommendations for action

The following recommendations can be derived from practical experience:

- **Start gradually:** begin with DMARC “none”, collect reports and learn.
- Tighten policies **gradually** and avoid sudden, comprehensive changes.
- **Use an analysis mailbox**: Set up a central collection point for reports.
- **Define processes**: Establish responsibilities for report analysis and DNS adjustments.
- **Use validation**: Employ tools such as MXToolbox or provider-specific portals.
- **Observe data protection**: Forensic reports may contain personal data.
- **Ensure transparency**: Keep management and IT regularly informed of progress.

Success factors

The company's successful roll-out since 2017 shows that:

- An iterative approach reduces risks and facilitates adjustments.
- Management support is crucial – particularly when it comes to safeguarding the brand’s reputation.
- Standard services provided by email providers significantly simplify technical implementation.
- Involve end users early on, for example by asking them to flag suspicious emails.
- Every day, the system automatically blocks thousands of spam and, in particular, phishing emails sent in the company’s name , enhancing security and reducing the internal workload.

Secure email communication is achieved through gradual technical hardening, transparent governance and continuous monitoring.

About the eco Association and the eco E-Mail Expert Group

eco – Association of the Internet Industry – is the largest Internet association in Europe, with around 1,000 member companies from over 70 countries. Since 1995, the eco Association has played a key role in shaping the development of the Internet, promoting new technologies and representing the interests of its members in political circles and international bodies. With offices in Cologne, Berlin and Brussels, the association is committed to fostering a high-performing and trustworthy digital infrastructure ecosystem. Its aim is to support the digital transformation of the economy and society based on democratic values and ethical digitalisation.

The **eco Association E-Mail Expert Group** deals with current developments in the field of email. As well as general topics, the focus is on technical content that is crucial for senders and recipients, and that influences their day-to-day business. The companies participating in the Expert Group generate the majority of email traffic in Germany and neighbouring European countries.

To operate successfully in this context, the Expert Group sees its role as establishing standards that cover all aspects of email and provide support for the smooth running of the respective business models. Many mechanisms that are now widely used have already emerged in the technical implementation of email.

Join the email network!

The E-Mail Expert Group of eco – Association of the Internet Industry is a technically oriented, closed working group. At three meetings a year, members discuss current issues and challenges relating to the operation of infrastructure for sending and receiving emails. We warmly invite you to help shape the future of email security together with us. You and your company will benefit in many ways by getting involved!!

Legal notice

eco – Association of the Internet Industry

Lichtstrasse 43h
50825 Köln
Germany

Tel.: +49 221 70 00 48-0

Email: info@eco.de

https://international.eco.de/

ams-OSRAM AG

Tobelbader Strasse 30
8141 Premstaetten
Austria

Phone: +43 3136 500-0

www.ams-osram.com

Authors of the study

Steffen Siguda, Patrick Koetter, Patricia Trinkaus

Layout and design: P. Trinkaus

Contact persons

Hauke Timmermann

Head of Digital Business Models – Member of the Managing Board

hauke.timmermann@eco.de

Patricia Trinkaus

Manager of Digital Business Models and Technologies

patricia.trinkaus@eco.de

Patrick Koetter

Leader of the eco Association E-Mail Expert Group

André Görmer

Leader of the eco Association E-Mail Expert Group

Disclaimer

This publication is intended solely for general information purposes and does not constitute legal or any other kind of professional advice. It cannot replace individual advice that takes into account the specific circumstances of each case. Although we have compiled the content with due care, we do not guarantee the accuracy, completeness or timeliness of the information. To the extent permitted by law, we exclude liability for any damage arising from the use of this publication, regardless of the legal basis.