

Inside Europe's Cyber Incidents 2026

One of the first regionally grounded analyses of incident data in Benelux and Germany

Eye Security collected data from 630 investigated incidents from small and medium-sized businesses in Benelux and Germany over a three-year period, of which 454 business email compromise (BEC) cases, 30 ransomware investigations, and 106 compromise assessments.

62%

of cases since Jan 2025 involved MFA bypass

70%

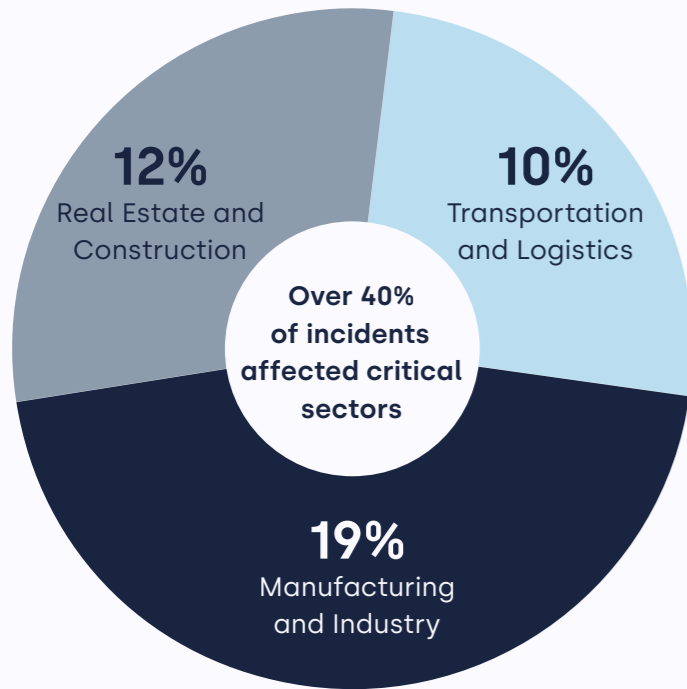
of all incidents were business email compromise (BEC)

40%

of BEC cases involved phishing

Most attacks were financially motivated, opportunistic, and scale-based, rather than highly targeted.

Critical industries under pressure



We are observing a shift toward industries that keep the economy moving. Production, logistics, and infrastructure are all on the radar now in a scenario where downtime equals leverage. Their dependence on continuous operations and narrow margins creates significant pressure to resume business quickly. Adversaries count on this pressure to increase their bargaining power.

However, most of the malicious activity we are dealing with is still driven by straightforward financial gain, with attackers starting out by "spray-and-pray" broad, opportunistic scans and mass-phishing to land those first compromises, rather than engaging in carefully tailored, highly targeted intrusions.

Lodi Hensen, VP Security Operations

Distribution of incidents per country

67.78%
Netherlands

17.78%
Belgium

8.41%
Germany

The MDR advantage



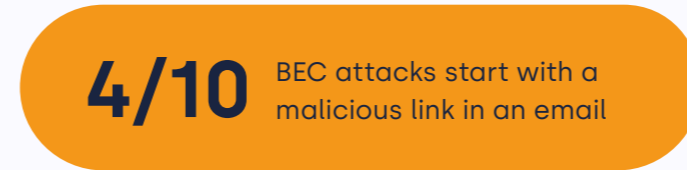
24 days



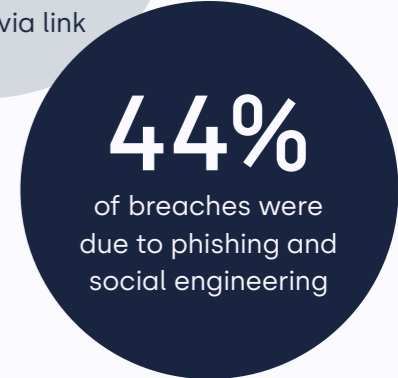
24 minutes
Reduction of median time BEC threat actors remained undetected in company networks

Attack landscape at a glance

Business email compromise



Main root causes were phishing links, attachment-based and service-based phishing. BEC was also the lead cause of recurring incidents within a year.



Ransomware



Compromise assessments



About Eye Security

Eye Security helps small and medium-sized businesses identify cyber risks proactively and strengthen operational resilience. As one of Europe's leading MDR providers, the company blends advanced AI technology, expert guidance, and integrated cyber insurance into one cohesive solution. More than 800 organisations across Europe rely on this unified approach to safeguard their digital operations.

www.eye.security



Incident response hotline

Experiencing a cyber incident? Call the Eye Security Incident Response hotline at +31 88 644 4898 (24/7 availability) or contact the IR team via email at cert@eye.security for non-urgent cases.

© 2026 Eye Security. All rights reserved. The information contained in this publication is provided for general informational purposes only and does not constitute any contractual or other form of commitment. While every effort has been made to ensure the accuracy and completeness of the content, Eye Security makes no guarantees regarding its correctness, completeness, or timeliness. Any liability, particularly for direct or indirect damages resulting from the use or non-use of this information, is excluded to the extent permitted by law. All service descriptions are subject to the applicable terms, exclusions, and conditions of the relevant contracts. This publication does not replace individual advice or contractual agreements.

