AIRNITE

ZERO DAY

ISSUE 13/2026 · IT SECURITY

Tense to critical: what Germany's BSI situation report 2026 means for companies

On 19 November 2026, Germany's BSI presented its annual situation report: 160 new vulnerabilities a day, attacks much faster after a flaw becomes known, SMEs and municipalities particularly vulnerable. The key figures and what to do now.

Published: 21 November 2026 Reading time: 5 min Author: Airnite editorial team

SOFTWARE. SECURITY. CODE.

// THE SITUATION IN NUMBERS

160
new vulnerabilities per day
35% more than the previous year (BSI, 19 Nov 2026)

8 days
to exploitation in Q2 2026
previously 53 and 25 days in the reporting periods (BSI)

+50%
rise in the BSI Cyber Index
average of 170 points, new indicator (BSI)

< 50%
users with basic protection
fewer than half use basic security measures (BSI)

Once a year, Germany's Federal Office for Information Security (BSI) reports on the state of IT security in the country. On **19 November 2026**, it presented its latest situation report – with a clear headline: the situation is **tense to critical**.

// What happened?

According to the BSI's press release, around **160 new vulnerabilities a day** are currently becoming known, 35% more than the previous year. The BSI has introduced a new **Cyber Index (BSI CX)**: it averaged 170 points, 50% higher than in the previous period.

The acceleration of attackers is particularly striking. According to the BSI, the time between a vulnerability becoming known and its exploitation fell from 53 days in the last reporting period to 25 days in the current one – and in the second quarter of 2026 to just **eight days**. Federal Interior Minister Alexander Dobrindt said at the presentation that Germany is a daily target of professional cyberattacks.

// How does the threat work?

BSI President Claudia Plattner describes a changed form of cyber aggression: faster, broader, more potent and much more complex. According to the BSI, AI-supported tools enable attacks at previously unknown volume and speed. Plattner stressed that security in cyberspace is not a state but has to be re-established again and again in a highly dynamic environment.

What this means in practice: if attackers exploit a new vulnerability after eight days on average, a monthly update cycle is no longer enough. Anyone operating systems reachable from the internet must install critical updates within a few days – or remove the exposure.

// Who is affected?

According to the BSI, **small and medium-sized enterprises and municipalities** are particularly vulnerable. They often have fewer staff for IT security but run the same systems as large organisations. Add to that a gap among users: according to BSI data, fewer than half of the users of digital services use basic security measures.

For companies this means: attacks are not just a risk for large corporations. Anything reachable on the internet gets scanned – and the time to react is getting shorter.

// What should you do now?

The core question from the report is: how quickly can you react? Companies should know their reachable systems, have an established process for critical updates and consistently implement basic protection. This includes multi-factor authentication, backups, training and a rehearsed emergency plan. The checklist below sums up the steps.

// How does Airnite help?

With **penetration tests** and an analysis of your attack surface, Airnite shows what is reachable and vulnerable from outside. In **consulting**, we build an update and emergency process with you that fits your size. In **training**, your staff learn to recognise phishing and AI-supported deception.

> Note: the figures come from the BSI's press release and overview page; we have not analysed the full report in detail. The report covers Germany. Research status: 21 November 2026.

Checklist: what to do now

[+] Know all systems reachable from the internet and remove unnecessary exposure.

[+] Set up a fixed process for critical updates that takes days rather than weeks – with owners and deputies.

[+] Subscribe to security alerts from authorities and vendors and have them assessed daily.

[+] Enforce basic protection everywhere: multi-factor authentication, up-to-date software, backups that survive an attack.

[+] Train staff regularly on phishing and AI-supported deception.

[+] Keep an emergency plan ready and rehearse it so everyone knows what to do.

How Airnite helps

- Penetration Testing & Security – Controlled attacks with a clear report and action plan.
- Consulting – An outside view of your plans and projects.
- Training – Your team learns our tools and processes.

Can you roll out updates within eight days?

Airnite checks how quickly critical updates are actually rolled out at your company, which systems are reachable from the internet and where basic protection is missing. You get a prioritised list of measures that fits your size – especially for SMEs and municipalities.

Request an initial call · Send an email · Via WhatsApp

Contact

Questions about this article? Message us on WhatsApp: +49 174 6834842

Read online: https://airnite.de/en/magazine/bsi-situation-report-2026-tense-to-critical/

Sources

Every fact in this article is based on the sources below. Primary sources are marked.

1. **BSI · Press release: BSI-Jahreslagebericht – Cybersicherheitslage in Deutschland ist angespannt bis kritisch** · 19 Nov 2026 · PRIMARY SOURCE
   Primary source: key figures, statements by the BSI President and the Federal Interior Minister
   https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2026/261119_Lagebericht.html
2. **BSI · Die Lage der IT-Sicherheit in Deutschland (overview)** · November 2026 · PRIMARY SOURCE
   Primary source: "tense to critical" assessment, BSI Cyber Index
   https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html

General editorial information, not legal advice and not an assessment of your individual systems. Status: date of publication.

Airnite GmbH · Am Waldbach 7 · 77654 Offenburg · airnite.de