AIRNITE

ZERO DAY

NUMÉRO 13/2026 · SÉCURITÉ INFORMATIQUE

De tendue à critique : ce que le rapport 2026 du BSI allemand signifie pour les entreprises

Le 19 novembre 2026, le BSI allemand a présenté son rapport annuel : 160 nouvelles vulnérabilités par jour, des attaques bien plus rapides après la découverte d'une faille, PME et collectivités particulièrement vulnérables. Chiffres clés et actions à mener.

Publié le: 21 novembre 2026 Temps de lecture: 5 min Auteur: Rédaction Airnite

SOFTWARE. SECURITY. CODE.

// LA SITUATION EN CHIFFRES

160
nouvelles vulnérabilités par jour
35 % de plus que l'année précédente (BSI, 19/11/2026)

8 jours
avant exploitation au T2 2026
contre 53 puis 25 jours sur les périodes de référence (BSI)

+50 %
hausse de l'indice cyber du BSI
moyenne de 170 points, nouvel indicateur (BSI)

< 50 %
utilisateurs avec protection de base
moins de la moitié appliquent des mesures de base (BSI)

Chaque année, l'Office fédéral allemand de la sécurité de l'information (BSI) fait le point sur la sécurité informatique en Allemagne. Le **19 novembre 2026**, il a présenté son dernier rapport – avec un titre sans ambiguïté : la situation est **tendue à critique**.

// Que s'est-il passé ?

Selon le communiqué du BSI, environ **160 nouvelles vulnérabilités par jour** sont actuellement rendues publiques, soit 35 % de plus que l'année précédente. Le BSI a introduit un nouvel **indice cyber (BSI CX)** : il s'est établi en moyenne à 170 points, 50 % de plus que sur la période précédente.

L'accélération des attaquants est particulièrement nette. Selon le BSI, le délai entre la publication d'une faille et son exploitation est passé de 53 jours sur la précédente période de référence à 25 jours sur l'actuelle – et à seulement **huit jours** au deuxième trimestre 2026. Le ministre fédéral de l'Intérieur, Alexander Dobrindt, a déclaré lors de la présentation que l'Allemagne était chaque jour la cible de cyberattaques professionnelles.

// Comment fonctionne la menace ?

La présidente du BSI, Claudia Plattner, décrit une cyberagression transformée : plus rapide, plus large, plus puissante et nettement plus complexe. Selon le BSI, des outils assistés par IA permettent des attaques d'un volume et d'une vitesse inédits. Claudia Plattner a souligné que la sécurité dans l'espace numérique n'est pas un état, mais doit être sans cesse rétablie dans un environnement très dynamique.

Concrètement : si les attaquants exploitent une nouvelle faille en huit jours en moyenne, un rythme mensuel de mises à jour ne suffit plus. Quiconque exploite des systèmes accessibles depuis Internet doit installer les mises à jour critiques en quelques jours – ou supprimer l'exposition.

// Qui est concerné ?

Selon le BSI, les **petites et moyennes entreprises ainsi que les collectivités** sont particulièrement vulnérables. Elles disposent souvent de moins de personnel pour la sécurité informatique, mais exploitent les mêmes systèmes que les grandes organisations. S'y ajoute une lacune côté utilisateurs : selon les données du BSI, moins de la moitié des utilisateurs de services numériques appliquent des mesures de protection de base.

Pour les entreprises, cela signifie que les attaques ne menacent pas que les grands groupes. Tout ce qui est accessible sur Internet est scanné – et le temps de réaction se réduit.

// Que faire maintenant ?

La question centrale du rapport est : à quelle vitesse pouvez-vous réagir ? Les entreprises doivent connaître leurs systèmes exposés, disposer d'un processus rodé pour les mises à jour critiques et appliquer systématiquement la protection de base : authentification multifacteur, sauvegardes, formations et plan d'urgence exercé. La check-list ci-dessous résume les étapes.

// Comment Airnite vous aide-t-il ?

Avec des **tests d'intrusion** et une analyse de votre surface d'attaque, Airnite montre ce qui est accessible et vulnérable depuis l'extérieur. En **conseil**, nous construisons avec vous un processus de mise à jour et d'urgence adapté à votre taille. En **formation**, vos équipes apprennent à reconnaître le phishing et les tromperies assistées par IA.

> Remarque : les chiffres proviennent du communiqué et de la page de présentation du BSI ; nous n'avons pas analysé le rapport complet en détail. Le rapport porte sur l'Allemagne. État de la recherche : 21 novembre 2026.

Check-list : ce qu'il faut faire maintenant

[+] Connaître tous les systèmes accessibles depuis Internet et supprimer toute exposition inutile.

[+] Mettre en place un processus fixe pour les mises à jour critiques, en jours plutôt qu'en semaines – avec responsables et suppléants.

[+] S'abonner aux alertes de sécurité des autorités et des éditeurs et les faire évaluer chaque jour.

[+] Imposer partout la protection de base : authentification multifacteur, logiciels à jour, sauvegardes résistant à une attaque.

[+] Former régulièrement les équipes au phishing et aux tromperies assistées par IA.

[+] Disposer d'un plan d'urgence et l'exercer pour que chacun sache quoi faire.

Comment Airnite vous aide

- Tests d'intrusion et sécurité – Attaques contrôlées avec rapport clair et plan d'action.
- Conseil – Un regard extérieur sur vos projets.
- Formations – Votre équipe apprend nos outils et méthodes.

Déployez-vous vos mises à jour en huit jours ?

Airnite vérifie la vitesse réelle de déploiement des mises à jour critiques chez vous, quels systèmes sont accessibles depuis Internet et où la protection de base fait défaut. Vous recevez une liste de mesures priorisée et adaptée à votre taille – notamment pour les PME et les collectivités.

Demander un premier échange · Écrire un e-mail · Par WhatsApp

Contact

Des questions sur cet article ? Écrivez-nous sur WhatsApp : +49 174 6834842

Lire en ligne: https://airnite.de/fr/magazine/rapport-bsi-2026-tendu-a-critique/

Sources

Chaque fait de cet article repose sur les sources ci-dessous. Les sources primaires sont signalées.

1. **BSI · Communiqué : BSI-Jahreslagebericht – Cybersicherheitslage in Deutschland ist angespannt bis kritisch** · 19/11/2026 · SOURCE PRIMAIRE
   Source primaire : chiffres clés, déclarations de la présidente du BSI et du ministre fédéral de l'Intérieur
   https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2026/261119_Lagebericht.html
2. **BSI · Die Lage der IT-Sicherheit in Deutschland (aperçu)** · novembre 2026 · SOURCE PRIMAIRE
   Source primaire : évaluation « tendue à critique », indice cyber du BSI
   https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html

Information éditoriale générale, sans conseil juridique ni examen individuel de vos systèmes. État : date de publication.

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