Responsabilité en matière de cybersécurité

LANCOM Systems considère les exigences relatives à des infrastructures informatiques sûres et fiables comme une condition fondamentale à la numérisation de l'économie et de l'administration publique. La cybersécurité constitue donc, depuis la création de l'entreprise, une partie intégrante du développement des solutions.

Le développement et l'assurance qualité des solutions LANCOM Systems sont réalisés en Allemagne conformément à des normes de sécurité élevées. Le label de qualité « IT Security made in Germany » de l'Association allemande pour la sécurité informatique (Bundesverband IT-Sicherheit), ainsi que les certifications de l'Office fédéral de la sécurité des technologies de l'information (BSI), attestent du niveau de sécurité atteint.
Les cyberattaques représentent un risque majeur pour les entreprises et les institutions publiques. Avec le Cyber Resilience Act, l'Union européenne a défini des exigences contraignantes en matière de cybersécurité pour les produits comportant des éléments numériques, créant ainsi un cadre réglementaire uniforme.
Bien que les exigences du Cyber Resilience Act (CRA) ne soient pleinement applicables qu'à partir de décembre 2027, LANCOM Systems intègre d'ores et déjà plusieurs dispositions essentielles du CRA dans le développement de ses solutions.

Ainsi, LANCOM Systems aligne la conception de ses solutions sur les principes suivants :

→ concevoir les solutions de manière à ce qu'elles offrent, même en présence d'interfaces externes, une surface d'attaque aussi réduite que possible (par exemple, limitation des identifiants d'accès dissimulés et des mécanismes de backdoor),

→ les développer de façon à ce que l'impact d'un incident de sécurité soit atténué grâce à des mécanismes et techniques appropriés (par exemple, éviter les mécanismes de chiffrement faibles),

→ et garantir que des informations liées à la sécurité soient fournies par l'enregistrement ou la surveillance d'événements internes pertinents, tels que l'accès aux données, aux services ou aux fonctions, ainsi que les modifications qui y sont apportées, tout en proposant aux utilisateurs un mécanisme d'opt-out.

Nous mettons en œuvre en continu des mesures techniques et organisationnelles complètes afin d'atteindre un niveau très élevé de cybersécurité pour nos solutions. Malgré toute la rigueur et notre engagement constant en faveur d'un niveau élevé de cybersécurité, une sécurité complète et constante ne peut être garantie. Un niveau de sécurité efficace repose non seulement sur des mesures techniques, mais également sur des processus organisationnels appropriés et leur mise en œuvre cohérente par les utilisateurs.

Würselen, le 23 mars 2026

Constantin von Reden,
CEO

Robert Mallinson,
Co-CEO