LANCOM SYSTEMS

Backdoor-Freiheits-Erklärung

Erklärung der LANCOM Systems GmbH

Produkte von LANCOM sind frei von versteckten Zugangsmöglichkeiten und sonstigen unerwünschten Funktionen zur Ein- und Ausleitung oder Manipulation von Daten.

LANCOM Systems weiß um die Bedeutung vertrauenswürdiger Infrastrukturen für die erfolgreiche Digitalisierung von Wirtschaft und Verwaltung. Eines der größten IT-Sicherheitsrisiken sind versteckte Zugangsmöglichkeiten (Backdoors) in Soft- und Hardware, die unbefugten Dritten das unbemerkte Eindringen in die Netze von Unternehmen, Behörden und Institutionen gestatten.

LANCOM verfolgt seit seiner Gründung eine konsequente Anti-Backdoor-Politik in seinem gesamten Produktportfolio. Das Kernportfolio wird gemäß höchsten Datenschutzstandards in Deutschland entwickelt und getestet. Das Qualitätszeichen **„IT-Security made in Germany“** (ITSMIG) und Zertifizierungen durch das Bundesamt für Sicherheit in der Informationstechnik bestätigen die Vertrauenswürdigkeit und das herausragende Sicherheitsniveau.

LANCOM Systems gewährleistet in diesem Zusammenhang die volle Übereinstimmung mit Ziffer 2.4 der Ergänzenden Vertragsbedingungen über den Kauf von Hardware (EVB-IT Kauf AGB), Version 2.0 vom 17.03.2016:

LANCOM Systems liefert die Hardware frei von Schaden stiftender Software, z. B. in mitgelieferten Treibern oder der Firmware (d. h. keine Viren, Würmer oder Trojaner). LANCOM Systems gewährleistet darüber hinaus, dass die von ihr zu liefernde Hardware frei von Funktionen ist, die die Integrität, Vertraulichkeit und Verfügbarkeit der Hardware, anderer Hard- und/oder Software oder von Daten gefährden und dadurch den Vertraulichkeits- oder Sicherheitsinteressen des Auftraggebers zuwiderlaufen durch

→ Funktionen zum unerwünschten Absetzen/Ausleiten von Daten,
→ Funktionen zur unerwünschten Veränderung/Manipulation von Daten oder der Ablauflogik oder
→ Funktionen zum unerwünschten Einleiten von Daten oder unerwünschte Funktionserweiterungen.

Insbesondere verpflichtet sich LANCOM Systems dazu, dass

→ in Produkten von LANCOM Systems keine geschwächten Verschlüsselungsmechanismen (z. B. durch künstlich verkürzte Schlüssel, inkorrekt implementierte Verschlüsselungsalgorithmen, geschwächte Zufallszahlengeneratoren, verdeckte Masterkeys oder im Datenstrom verdeckt übertragene Informationen, die eine Entschlüsselung erleichtern) Anwendung finden,
→ Produkte von LANCOM Systems keine verdeckten Zugangskennungen, Zugangsmechanismen oder andere dem Unternehmen bekannte Umgehungswege enthalten, die Dritten einen vom Kunden nicht kontrollierten Zugriff ermöglichen oder sicherheitsrelevante Funktionen deaktivieren.

Würselen, 14. November 2024

Ralf Koenzen
Geschäftsführer LANCOM Systems

Christian Schallenberg
CTO LANCOM Systems