bintec elmeg
MAKING THE NET WORK

WLAN WPA2 Schwachstelle

Warum bintec elmeg Geräte NICHT betroffen sind.

Am 7.8.2018 berichteten Medien von einer neuen Angriffsmethode auf WLAN Access Points, deren Verbindungen mittels WPA2 PSK verschlüsselt werden.
WLAN-Produkte, deren Verbindungen mittels WPA2 Enterprise absichert sind, sind von dieser Angriffsmethode nicht betroffen.

Ebenso wenig greift die Angriffsmethode bei bintec elmeg WLAN-Produkten, die mit WPA Personal abgesichert sind. Diese wenden das Pairwise Masterkey Caching (PMK), bei dem die Methode ansetzt, nicht an.

Darüber hinaus können Access Points mit folgenden Maßnahmen effizient vor einer Ausnutzung der Angriffsmethode geschützt werden:

- Die Kombination von WPA2 und der Verschlüsselung der gesendeten Daten mit dem als unsicher geltenden TKIP sind zu vermeiden.
- WLAN-Passwörter müssen ausreichend lang und komplex gewählt werden.
- Im Auslieferungszustand voreingestellte Passwörter müssen einmalig sein und den o.g. Sicherheitsansprüchen genügen.

Alle diese Maßnahmen werden von Geräten der bintec elmeg GmbH unterstützt:

- Die Kombination von WPA2 und TKIP wird nicht als Standardeinstellung verwendet.
- Die Eingabe eines ausreichend langen Passwortes wird erzwungen, auf die Notwendigkeit eines komplexen Passwortes wird hingewiesen.
- Geräte, deren Drahtlosnetzwerke ab Werk aktiviert sind, verfügen über ein individuell generiertes, langes Passwort.

bintec elmeg

bintec elmeg GmbH
Südwestpark 94
D-90449 Nürnberg
www.bintec-elmeg.com