

Die unterschätzte Sicherheitslücke im Büro

WARUM TASTATUREN UND MÄUSE EIN TEIL
DER IT-SECURITY SIND UND WAS MODERNE
TECHNOLOGIEN HEUTE BESSER MACHEN.



SICHERE ARBEITSPLATZLÖSUNGEN FÜR MODERNE BÜROS

Kann Ihre Tastatur gehackt werden?

Kann Ihre Tastatur gehackt werden?

Viele Unternehmen investieren viel in IT-Sicherheit: Firewalls, sichere Cloud-Lösungen, Backup-Strategien und Zugriffskontrollen. Doch ein möglicher Schwachpunkt wird im Büroalltag häufig übersehen: die Peripheriegeräte am Arbeitsplatz.

Drahtlose Tastaturen und Mäuse kommunizieren über Funk mit dem Computer. Wenn diese Funkverbindungen nicht ausreichend geschützt sind, können sie theoretisch zu einem Sicherheitsrisiko werden.

Darum lohnt sich auch bei Tastatur und Maus ein Blick auf die eingesetzte Technologie.



SICHERE ARBEITSPLATZLÖSUNGEN FÜR MODERNE BÜROS

Das unterschätzte Risiko

Das unterschätzte Risiko

Tastaturen und Mäuse übertragen täglich sensible Informationen, zum Beispiel:

- Passwörter und Logins
- E-Mails und Dokumente
- Zugänge zu Cloud-Systemen
- interne Geschäftsdaten

Bei drahtlosen Geräten werden diese Eingaben über Funk an den Computer übertragen. Wenn eine Verbindung nicht ausreichend geschützt ist, könnten Angreifer unter bestimmten Umständen versuchen, Funksignale abzufangen oder Geräte zu manipulieren. Besonders ältere oder sehr günstige Geräte verfügen teilweise über veraltete Sicherheitsmechanismen.



SICHERE ARBEITSPLATZLÖSUNGEN FÜR MODERNE BÜROS

Welche Daten übertragen Tastaturen?

Früher ein reales Problem

Bei frühen drahtlosen Tastaturen und Mäusen lag der Fokus vor allem auf Komfort – weniger auf Sicherheit.

Typische Schwachstellen waren zum Beispiel:

- keine oder nur sehr einfache Verschlüsselung
- fehlende Authentifizierung zwischen Gerät und Empfänger
- unsichere oder offene Pairing-Mechanismen

Sicherheitsforscher konnten deshalb in einigen Fällen Tastatureingaben aus der Distanz mitlesen.

Diese Erkenntnisse haben dazu geführt, dass Hersteller ihre Funktechnologien und Sicherheitsmechanismen in den letzten Jahren deutlich verbessert haben.



SICHERE ARBEITSPLATZLÖSUNGEN FÜR MODERNE BÜROS

Warum ältere Geräte unsicher sein können

Moderne Business-Peripherie

Moderne Geräte für den professionellen Einsatz setzen heute auf deutlich höhere Sicherheitsstandards.

Dazu gehören unter anderem:

- verschlüsselte Funkübertragung zwischen Gerät und Computer
- authentifizierte Verbindung zwischen Tastatur, Maus und Empfänger
- kontrollierte und sichere Geräte-Kopplung (Pairing)

Ein Beispiel dafür ist Logitech Logi Bolt.

Diese Funktechnologie wurde speziell für professionelle Arbeitsplätze und Unternehmen entwickelt. Sie kombiniert eine stabile Verbindung mit modernen Sicherheitsmechanismen.



SICHERE ARBEITSPLATZLÖSUNGEN FÜR MODERNE BÜROS

Moderne Sicherheitsstandards

Verschlüsselung und FIPS

Die Logi Bolt Technologie ist vollständig verschlüsselt und FIPS-kompatibel.
FIPS steht für Federal Information Processing Standards.

Dabei handelt es sich um Sicherheitsrichtlinien für kryptografische Verfahren, die vom National Institute of Standards and Technology (NIST) in den USA definiert werden.

Diese Standards legen fest, wie Verschlüsselung, Authentifizierung und Schlüsselverwaltung umgesetzt werden müssen, damit sie als sicher gelten.

Technologien, die diese Anforderungen erfüllen, eignen sich besonders für Organisationen mit erhöhten Sicherheitsanforderungen.



SICHERE ARBEITSPLATZLÖSUNGEN FÜR MODERNE BÜROS

Fazit

Cybersicherheit endet nicht beim Netzwerk oder beim Server.
Auch Geräte wie Tastaturen und Mäuse sind Teil der gesamten Sicherheitsarchitektur eines modernen Arbeitsplatzes.

Unternehmen sollten deshalb darauf achten:

- dass drahtlose Geräte verschlüsselte Funktechnologien verwenden
- dass eine sichere Geräte-Kopplung gewährleistet ist
- dass Business-Hardware statt einfacher Consumer-Geräte eingesetzt wird

Wir beraten Sie gerne bei der Auswahl von sicheren Tastaturen, Mäusen und modernen Arbeitsplatzlösungen für Ihr Unternehmen.



SICHERE ARBEITSPLATZLÖSUNGEN FÜR MODERNE BÜROS