

# WEP (Wired Equivalent Privacy)

**WEP** je historicky první bezpečnostní algoritmus pro bezdrátové síť Wi-Fi ([WLAN](#)), uvedený v roce 1997 jako součást standardu IEEE 802.11. Jeho cílem mělo být poskytnutí stejné úrovně soukromí, jakou nabízí drátová síť, ale kvůli zásadním kryptografickým chybám je dnes považován za **zcela nepoužitelný a nebezpečný**.

## Proč je WEP nebezpečný?

Zabezpečení WEP trpí několika fatálními slabiny, které umožňují útočnickovi proniknout do sítě během několika minut:

- **Slabé šifrování:** Používá proudovou šifru RC4 s krátkými a statickými klíči.
- **Krátký inicializační vektor (IV):** 24bitový IV je příliš krátký, což vede k jeho častému opakování. Útočník může sběrem dostatečného množství paketů zpětně vypočítat síťový klíč.
- **Snadné prolomení:** Existují volně dostupné nástroje (např. Aircrack-ng), které dokáží WEP heslo zjistit automatizovaně i bez znalosti administrátorských údajů.

## Srovnání standardů

V naší síťové architektuře se striktně držíme modernějších nástupců:

Standard	Stav	Bezpečnostní status
<b>WEP</b>	Zastaralý (Deprecated)	<b>Kriticky nebezpečný</b>
<a href="#">WPA</a>	Zastaralý	Nedostatečný
<a href="#">WPA2</a>	Standard	Vysoká (při použití AES)
<a href="#">WPA3</a>	Doporučený	Maximální

## Striktní pravidla pro firmu

V rámci naší strategie [kybernetické bezpečnosti](#) platí následující omezení:

- **\*\*Zákaz nasazení:\*\*** Žádný přístupový bod (AP) v naší síti nesmí mít aktivované šifrování WEP.
- **\*\*Audit zařízení:\*\*** Starší zařízení, která podporují pouze WEP, nesmějí být připojována do firemní sítě. Pokud je jejich provoz nezbytný (např. staré skladové terminály), musí být izolována v samostatné VLAN bez přístupu k internetu a interním datům.
- **\*\*Domácí síť ([[Práce na dálku|Home Office]]):\*\*** Zaměstnanci pracující z domova nesmí používat routery nastavené na WEP. Pokud vaše domácí zařízení WEP stále používá, kontaktujte [\[\[IT Podpora|IT podporu\]\]](#) pro konzultaci nákupu nového vybavení.

## Jak poznat WEP?

Při připojování k Wi-Fi se v operačním systému Windows nebo macOS zobrazí varování: „Tato síť používá zastaralý standard zabezpečení, který vás vystavuje riziku.“\* V takovém případě se k síti **nepřipojujte**.

**Historická poznámka:** WEP byl oficiálně nahrazen standardem WPA již v roce 2003, přesto se s ním v terénu u špatně nastavených zařízení stále můžete setkat.

— **Související stránky:** [Kybernetická bezpečnost](#), [WLAN](#), [WPA](#), [IT Podpora](#), [Práce na dálku](#)

From:

<http://serviceit.cz/> - **IT ENCYKLOPEDIA**

Permanent link:

<http://serviceit.cz/doku.php?id=wep>

Last update: **2026/01/01 15:53**

