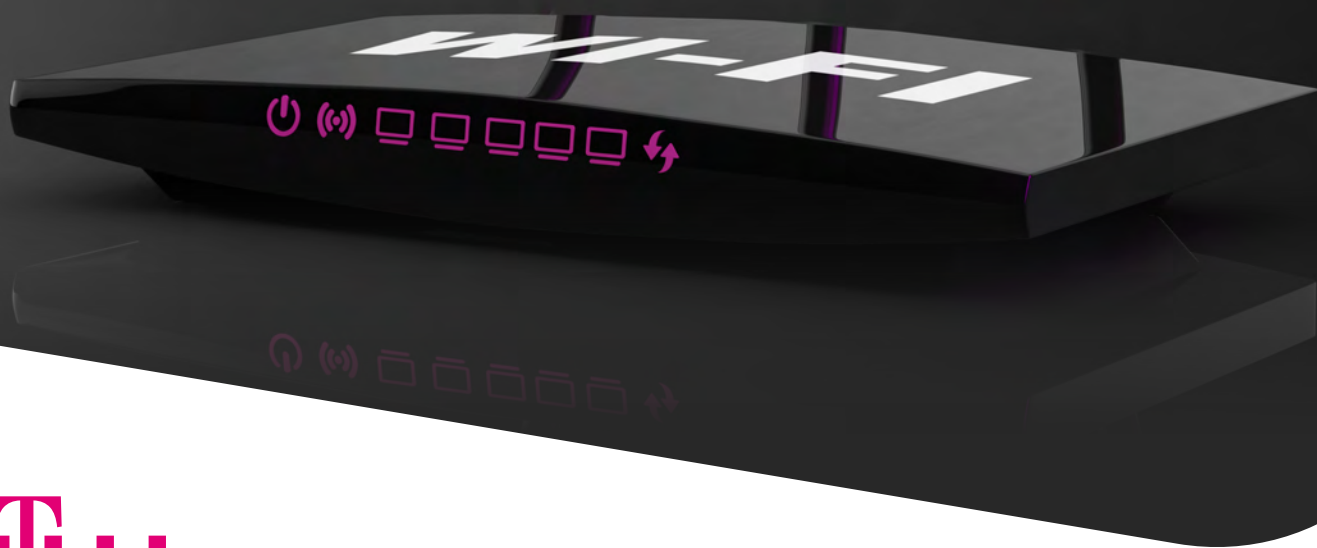


IT:Works

10

Desatoro pre bezpečnú sieť



T . .

10 štandardov pre bezpečnú firemnú sieť pre rok 2022

Má vaša spoločnosť viac pobočiek, externé tímy alebo veľké priestory a podujatia s veľa návštevníkmi? To všetko sú scenáre, kedy je dôležité vytvoriť skutočne zabezpečenú sieť a ochrániť komunikáciu a citlivé dáta.

Aké bezpečnostné opatrenia by mala spĺňať firemná sieť, ktorá dokáže odolávať sofistikovaným kybernetickým útokom?

Prečítajte si odporúčania, čo všetko by mala spĺňať skutočne zabezpečená sieť, ktoré sme pripravili s našimi odborníkmi:

1. Celá firemná komunikácia by mala byť kryptovaná.**2. Akýkoľvek prístup na Internet by mal prechádzať cez security zariadenie (NG Layer7 Firewall, UTM):**

- Intrusion Defense System (IDS) functionality – funkcionálnosť systému obrany proti vniknutiu (IDS).
- Intrusion Prevention System (IPS) functionality – funkcionálnosť systému prevencie narušenia (IPS).
- Service and traffic functionality tools – nástroje funkčnosti služieb a premávky.

3. Akýkoľvek vzdialený prístup do firemnej siete by mal byť kryptovaný a užívateľ musí byť autentifikovaný.

- Strong Virtual Private Network (VPN) data encryption – silné šifrovanie dát virtuálnej súkromnej siete VPN.

4. Každý by mal mať prístup iba k dátam, ktoré potrebuje – Zero Trust Network Policies.

Vďaka Dashboardu spoznáte online preferencie svojich zákazníkov – ako sieť používajú, aké stránky navštevujú a prispôbiť ich preferenciám svoje marketingové aktivity.

5. Sieť by mala poskytovať aplikovanú správu a manažment prístupov a zariadení.**6. Wi-Fi sieť by mala byť vždy kryptovaná aktuálne dostupnou metódou.****7. Wi-Fi sieť pre hostí by mala byť oddelená, aby ste ochránili svoje citlivé firemné dáta.****8. Sieť by mala chrániť koncové zariadenia:**

- AV Scanning – antivírusová ochrana
- Malware Scanning – skenovanie škodlivého softvéru
- IP reputation awareness – povedomie o povesti IP
- Dynamic URL categorization techniques – techniky kategorizácie dynamických adries URL
- Data leakage prevention function – funkcia prevencie úniku dát

9. Sieť by mala dovoliť logovanie a auditovanie sieťovej aktivity.**10. Na kontrolu sieťovej aktivity by mal byť implementovaný SOC.**

Skutočne zabezpečená firemná sieť musí spĺňať viacero atribútov, ktoré sú nevyhnutné na to, aby boli citlivé dáta chránené v každej fáze komunikácie a spracovania. Je dôležité nič nepodceniť – každý diel skladačky sa podieľa na celkovej bezpečnosti firemnej siete.

O IT:Works

IT:Works poskytuje komplexné IT služby pre maximálne využitie konektivity. Umožňuje vytvoriť firemnú sieť a bezpečne prepája pobočky, zamestnancov aj návštevníkov. Pri špecifických požiadavkách poskytujeme službu CloudNet – riešenie na mieru.

Spojte sa s naším špecialistom a zistite viac o tom, ako IT:Works môže pomôcť vytvoriť zabezpečenú sieť aj pre vašu firmu. Zarezerwujte si dátum a čas, ktoré Vám vyhovujú.

Vybrať termín

☎ 0800 123 500



Managed Security Box a Wi-Fi pre rôzne veľké firmy



Managed Security Box

Pre maximálne využitie vašej siete, ochranu citlivých dát, riadenie využívania siete, bezpečný home office a VPN pripojenie.

od 66 €
bez DPH mesačne*

Mám záujem



Managed Wi-Fi S

Vhodná do vnútorných priestorov, pre malé kancelárie, obchody, prevádzky, predajne a služby.

od 26 €
bez DPH mesačne*

Mám záujem



Managed Wi-Fi M

Dvakrát väčší dosah než Wi-Fi S - vhodná do vnútorných priestorov pre malé, stredné firmy a kancelárie.

od 30 €
bez DPH mesačne*

Mám záujem



Managed Wi-Fi L

Vhodná aj do exteriérov – vysporiada sa s rôznymi poveternostnými podmienkami, pre kaviarne, reštaurácie, hotely, eventy, festivaly, pláže a vonkajšie objekty.

od 32 €
bez DPH mesačne*

Mám záujem



Máte špecifické potreby?

Využite **CloudNet** – riešenie na mieru.

Mám záujem