CTI Jelentés

Otthoni hálózatok biztonsága

NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NEMZETI KIBERVÉDELMI INTÉZET

Tartalomjegyzék

1. Bevezetés 3

2. Az átlagos otthoni hálózat felépítése 5

3. A biztonság fontossága és bevett gyakorlatok 9

4. Alapvető router beállítások 10

Bevezetés

Gyakran bele se gondolunk, hogy manapság mennyire természetessé és magától értetődővé vált az állandó és folyamatos internetkapcsolat. Legyen szó az otthoni, a munkahelyi vagy a tömegközlekedésen történő internetezésről, **elvárt lett a gyors internetkapcsolat**. Amíg korábban a webes tartalmak összetétele miatt elegendő volt egy jóval lassabb hálózati sebesség, addig manapság a több száz Mbps-os sebesség szükséges a zökkenőmentes internetezéshez. A **pandémiás időszak felgyorsította a digitalizációs folyamatokat**, amihez szintén nélkülözhetetlen a megfelelő internetkapcsolat. A Központi Statisztikai Hivatal adatai szerint 2020-ban a magyar háztartások 88%-a rendelkezett internethozzáféréssel, valamint a ranglistákon Magyarország az átlagos internetsebességet tekintve a 10 legjobb ország között volt. Az internet olyannyira fontos és szerves részévé vált az életünknek, hogy gyakran már az óvodáskorú gyermekek is használják különböző eszközökön.

Az interneten keresztül végezzük a munkánkat, banki tranzakcióinkat, magánbeszélgetéseinket, de ezen keresztül ellenőrizzük az otthoni biztonsági kameráinkat, vagy állíthatjuk be a fűtés hőfokát. Csak gondoljunk bele milyen kiszolgáltatottnak érezhetjük magunkat, ha egy elavult router firmware vagy gyenge Wifi jelszó által kompromittálódik mindaz, amely a privát életünk része.

Az internethasználat számos veszélyt rejt önmagában. Ennek eredendő forrásai lehetnek a nem megfelelően konfigurált hálózati eszközeink. A nyílt internet felől csak akkor tudnak hívatlan vendégek hozzáférni az otthoni hálózatunkhoz, ha hagyjuk azt. Jelen dokumentumban a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet olyan **javaslatokat és jó gyakorlatokat fogalmaz meg** a felhasználók számára, amivel biztonságossá tehetik az otthoni hálózatukat, hogy megvédjék a nyílt internet felől származó veszélyektől önmagukat és családtagjaikat.

Az átlagos otthoni hálózat felépítése

A biztonságos hálózat kialakítása érdekében elsősorban meg kell ismernünk, hogy a hálózatunk milyen elemekből épül fel. Az internet egy helyi szolgáltató (Internet Service Provider - ISP) által kerül bevezetésre az otthonokba. Ezek lehetnek országos méretűek (például Telekom, Digi), vagy lehetnek olyan kisebb szolgáltatók, amelyek jellemzően csak egy-egy megyében vagy adott esetben csak néhány településen érhetők el. A szerződés megkötése után az adott ISP egy modem-et biztosít számunkra, amit a technikus beüzemel az internetbekötés során.

A **modem a külső hálózat felé jelent alapértelmezett átjárót**, avagy linket, amely kapcsolatot biztosít a belső eszközeink számára az internettel. Általánosságban megszokott, hogy a szolgáltató által nyújtott modemek több hálózati eszközt vagy funkciót is magukba foglalnak, mint pl. a router, switch, és vezetéknélküli elérésipont (Wireless Access Point) avagy ahogy sokan ismerjük a Wi-Fi. Így a modem beüzemelését követően a felhasználó bármiféle egyéb beállítás vagy új eszköz beszerzése nélkül **képes elérni a világhálót**.

Jobb teljesítmény, nagyobb WiFi lefedettség, vagy egyéb kiegészítő funkciók érdekében azonban széles választékból szerezhető be **vezeték nélküli router** (wireless router) is. Ez az eszköz ethernet kábel segítségével összeköttetésbe kerül a modemmel és a saját antennáin vagy beépített portjain keresztül képes otthonunk különböző eszközeinek biztosítani az internet kapcsolatot. Ez a technológia megadja a szabadságot a hordozható eszközök nagysebességű internetelléréséhez.

A stabilabb internetkapcsolat mellett egy ilyen eszköz **jóval több biztonsági funkcióval és beállítási lehetősséggel rendelkezik**, mint a szolgáltatótól kapott modem.

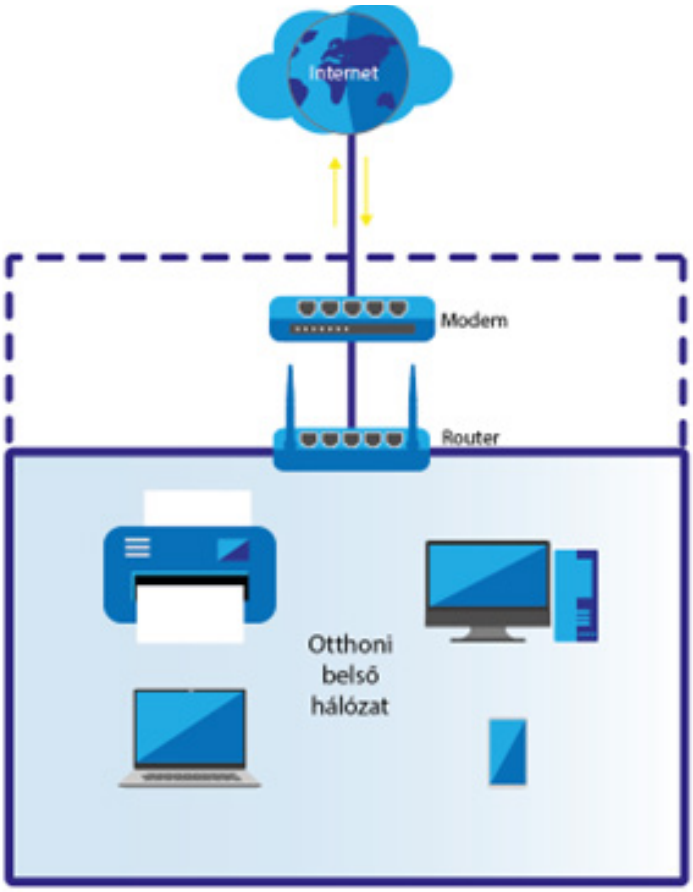
Említésre érdemesek a napjainkban egyre szélesebb körben elterjedő hordozható **Wi-Fi hotspotok** is. Ez a megoldás a mobil internet kapcsolatát osztja meg helyi elérésű Wi-Fi protokollon keresztül. Főleg olyan háztartásokban használatos, ahol a vezetékes internet bekötés nem lehetséges, de remekül funkcionál utazás vagy nyaralás esetén, amikor nincs elérhető vezetékes internet.

A Wifi mellett megjelennek más hálózati technológiák is mint a **Bluetooth**, **Zigbee** és **Z-Wave**. Sokszor találkozhatunk ezekkel a protokollokkal IoT okos eszközöknél, de akár fejhallgatóknál, hangszóróknál is. A Wi-Fi-vel szemben mindhárom technológia kis energiafelhasználású, ezért tökéletes hordozható készülékekhez.

Összefoglalva tehát, az otthoni hálózatunk legfontosabb elemei: a modem és a router. Azonban a hálózatunknak lehetnek más, általunk nap, mint nap használt eszközei is. A legelterjedtebb internetre csatlakoztatható eszközök, amelyek egy háztartásban általában megtalálhatók:

- Számítógép (PC, laptop)
- Mobiltelefonok
- Tabletek
- Nyomtatók
- Játékkonzolok
- TV, TV-box
- Okos eszközök
- Biztonsági kamerák, babamonitor

Az IoT vagy okoseszközök egyre csak fejlődő világa az otthoni automatizációt forradalmasítják. Olyan eszközöket is magába foglalnak, mint kapucsengők, légtisztítók, biztonsági kamerák, órák, LED izzók, termosztátok, hangszórók stb. Közös jellemzőjük, hogy helyi hálózatot kialakítva képesek lehetünk különböző funkciókat irányítani a mobileszközünkről. A távirányítás, programozhatóság, időzítés, távoli felügyelet mind olyan előnyök, amelyekkel könnyebbé, precízebbé és irányíthatóbbá tehetjük életünket. Az előny gyakran hátránnyal is jár, amely ebben a kategóriában az **eszközök sérülékenységeivel** érkezik. Az IoT eszközök könnyen áldozatul eshetnek a kiberbűnözők káros tevékenységeinek, amellyel többek között betekintést nyerhetnek az otthoni privát életünkbe. Az okoseszközök biztonsági témakörében részletesebben olvashatnak az NBSZ NKI hamarosan megjelenő „IoT eszközök biztonsági kérdései" jelentésében.



1. ábra Általános otthoni hálózat sematikus ábrája

A fenti hálózati diagrammon is jól látható, hogy a router mint egy kapu szeparálja, de közben kapcsolatban is tartja a külső internetet a belső otthoni eszközeinktől. **Minden webes kérés ezen az interfészen keresztül halad át** és biztosítja a mi internetes biztonságunk alapját. Olyan biztonsági eszközöket nyújt nekünk a dobozból kivéve mint Tűzfal, hálózati címfordítás, port blokkolás, vendég hálózat stb.

A biztonság fontossága és bevett gyakorlatok

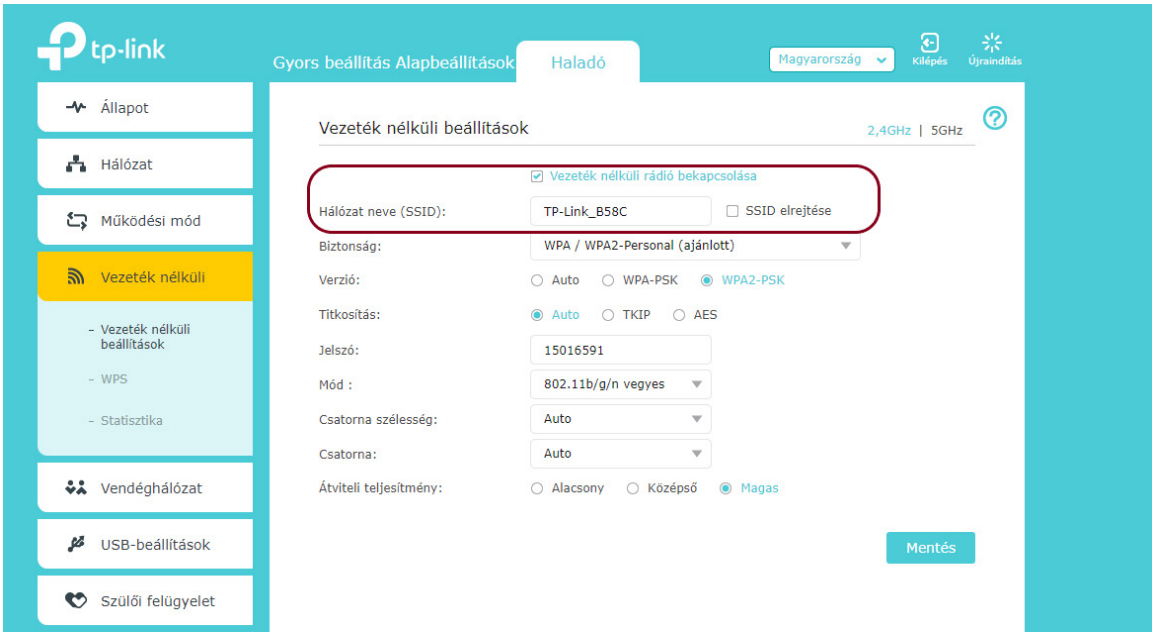
Sok emberben él az a téveszme, hogy ők túlságosan „kicsik" ahhoz, hogy érdekeljék a kiberbűnözőket. Sajnos a valóság nem ezt mutatja. Az NBSZ NKI fontos küldetésnek tartja, hogy felkeltse az emberek igényét arra, hogy **tudatosan végezzék az informatikai és internetes tevékenységeiket**. Ehhez nyújtanak segítséget a következőkben felsorolt egyszerű, kevés erőfeszítést igénylő, bevált jó gyakorlatok. A következő beállítási javaslatokhoz egy Tp-link Archer C7 Wi-Fi router kezelő felületéről készültek képernyőképek, amelyek támpontot adhatnak arról, hogy az egyes beállításokat milyen menüpont alatt lehet megtalálni.

Alapvető router beállítások

A következő beállításokat könnyedén elvégezhetjük a routerünkön, egy böngészőben megnyitott portálon keresztül. Ez a portál elérhető a böngésző kereső mezőjébe beírt cím alapján. Ez a gyártótól függően bármi lehet (érdemes a megvásárolt eszköz dobozán vagy leírásában megkeresni), de általában a 192.168.0.1 vagy 192.168.1.0 címeken elérhetőek. Új router vásárlása esetén érdemes olyan eszközt választani, amely rendelkezik mobiltelefonra letölthető applikációval. Ez egyszerűbbé teszi a beállításokat, emellett értesítéseket kaphatunk olyan információkról is, mint például elérhető szoftverfrissítések vagy hívatlan felcsatlakozott eszközök.

Hálózat név megváltoztatása

Hálózati eszközünk beszerelésekor és üzembehelyezésekor az alapvető **gyárilag beállított vezeték nélküli hálózati névvel (SSID) és jelszóval** jön létre a Wifi kapcsolatunk. Ezen adatok gyakran a gyártóhoz köthető információval vagy felismerhető sémával jönnek létre, amely a kiberbűnözőknek esélyt ad a modem vagy router modell és az azokhoz tartozó esetleges sérülékenységeknek megállapításához. Érdemes olyan SSID-t választani, amely semmiféleképpen nem köthető hozzánk, és nem árul eé rólunk információt. Amennyiben ennél is tovább szeretnénk menni felmerülhet a **SSID elrejtése** is. Ezáltal a készülékünk által elérhető Wi-Fi hálózatok között „Rejtett Hálózat" néven jelenik meg a saját hálózatunk. Ebben az esetben a felcsatlakozáshoz tartozó felugró ablak nem csupán a jelszót kéri, hanem a hálózat nevét is. A két autentikációs információ kitalálása drasztikusan megnehezíti a rosszindulatú szereplők dolgát.



2. ábra Hálózati név (SSID) megváltoztatása vagy elrejtése.

Jelszó megváltoztatása

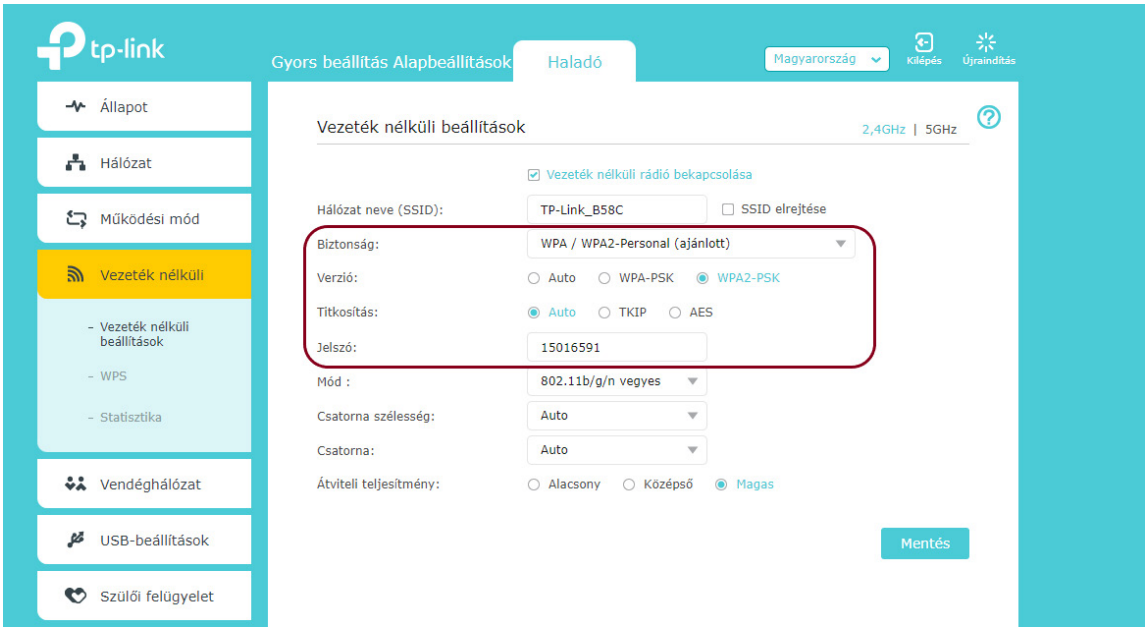
Hasonlóan az előző ponthoz fontos lépés a routerhez tartozó **gyári jelszó megváltoztatása**. A router gyárójának ismeretében gyakran kikövetkeztethető az alapértelmezett jelszó, amely esélyt adhat a támadóknak arra, hogy hálózatunkra bejutva kárt okozzanak. Ajánlott **legalább 12 karakteres, számot, kis és nagybetűt, speciális karaktereket vegyesen tartalmazó, ránk nem jellemző jelszót választani**. Érdemes a jelszógenerálásához és tárolásához **jelszószéfet** használni, amely megkönnyíti a jelszavak biztonságos kezelését.

Router kikapcsolása

Amennyiben elutazunk huzamosabb időre vagy akárcsak pár napra üresen hagyjuk otthonunkat érdemes áramtalanítani a routert. Ezzel nem csak az energia számlát csökkenthetjük, de a hívatlan internetes betolakodókat is megspórolhatjuk magunknak.

Erős Wi-Fi titkosítási protokoll beállítása

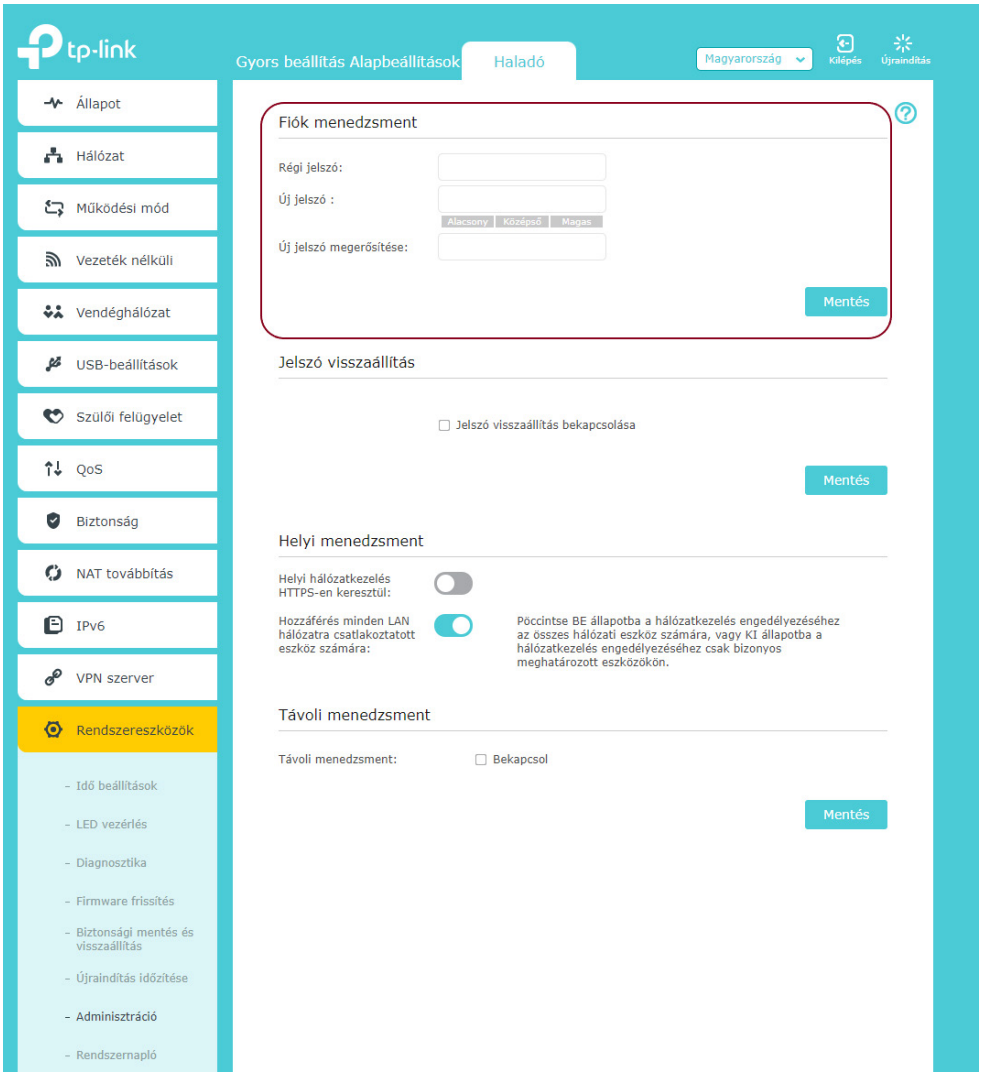
A vezeték nélküli hálózatunk jelerőssége gyakran akkora, hogy otthonunkon kívül is elérhető (például egy panelházban több tucat hálózatra tudnánk csatlakozni az egyes lakásokban a megfelelő információk tudatában). Ezért is fontos, hogy olyan **titkosítással rendelkezzen** a Wi-Fi hálózatunk, amely biztosítja, hogy a két fél közötti kommunikáció (mobil eszközünk és a Wi-Fi router) megbízható és titkos csatornákon megy, és más nem tudja azt lehallgatni a kommunikációs forgalomba való közbeékelődéssel. Az elérhető és beállítható protokollok lehetnek a WEP, WPA, WPA 2, WPA 3. Sajnos az első kettő (WEP, WPA) könnyű feltörhetőségük miatt már elavult technológiának számítanak, ezért ezek használata nem ajánlott. A router böngészőben megnyitható beállítási felületén találhatjuk a WPA beállításokat, ahol válasszuk a WPA 2 vagy WPA 3 protokollokat AES titkosítási algoritmussal.



3. ábra Wifi kommunikáció titkosítási protokol beállítása.

Router admin felhasználónév és jelszó megváltoztatása

A router beállításaihoz használt böngészőben megnyitható felhasználói felület kritikus beállítási lehetőségeket tartalmaz. Ezért is fontos, hogy az ehhez tartozó **alapértelmezett felhasználónevet és jelszót** az előzőkéhez hasonlóan **mindenképpen változtassuk meg**.

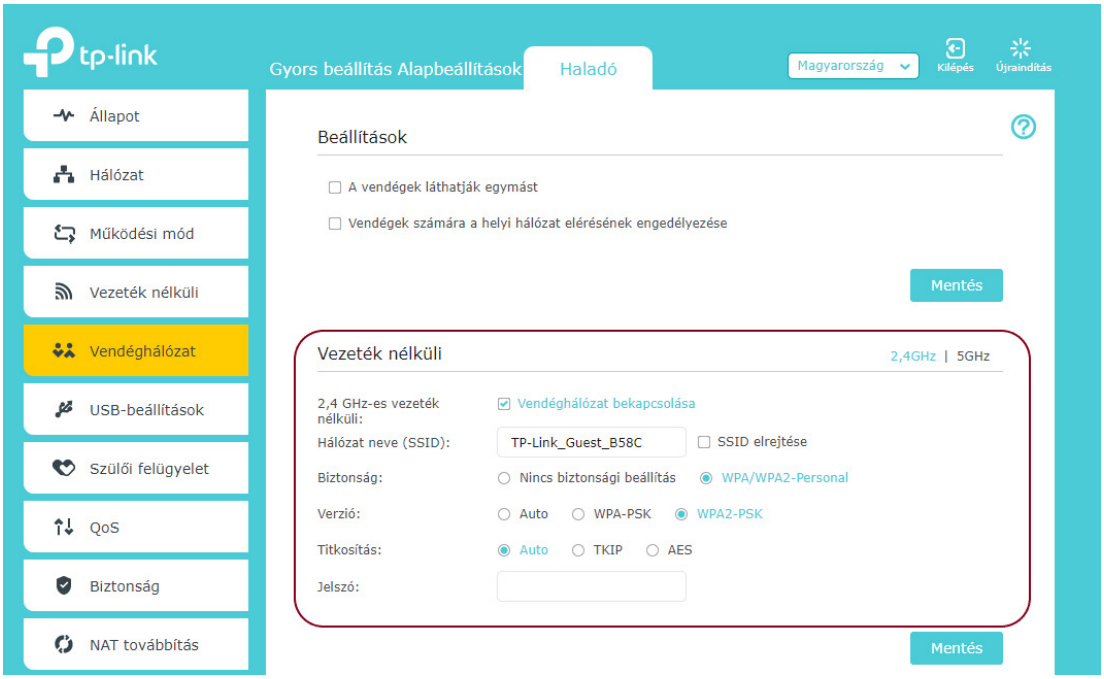


4. ábra Adminisztrátori jelszó megváltoztatása

Külön hálózat kialakítása vendégeknek és IoT eszközöknek

Vendégeinknek gyakran szükségük lehet internet elérésre, viszont bármennyire is megbízunk bennük, eszközeik a tudtukon kívül is tartalmazhatnak olyan káros kódokat, programokat, amelyek az otthoni hálózatunkba bejutva, képesek megfertőzni saját eszközeinket is. Az informatikában bevett gyakorlat a **hálózatok elválasztása** (hálózat szeparáció). A mai routereken és modemeken már pár kattintással kialakítható egy **vendéghálózat**, ami lehetővé teszi, hogy az erre csatlakozott eszközök ne lássanak rá a privát megbízható hálózatunkra.

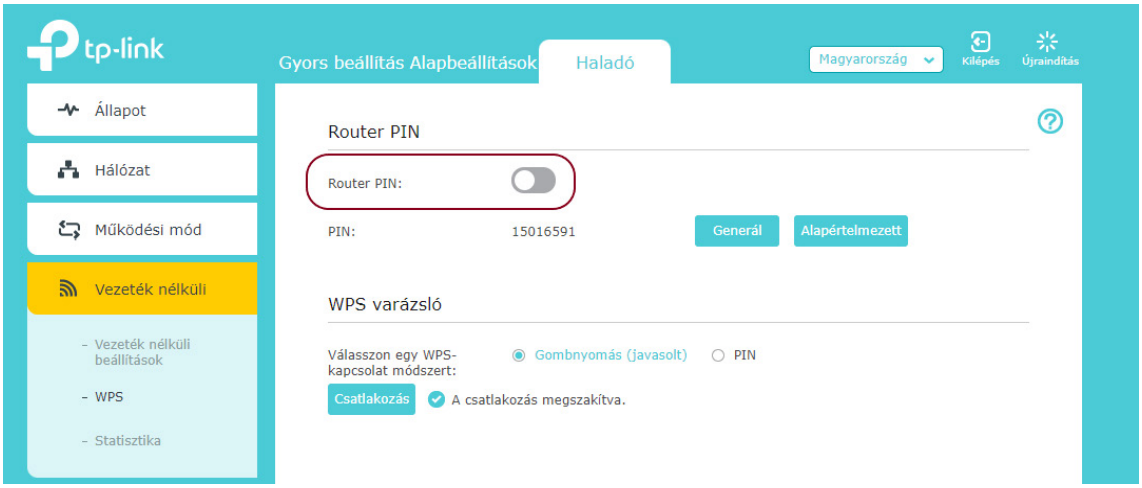
Az IoT és okoseszközök esetén a gyártók a termék gyorsabb és olcsóbb előállítása, az eladási ár csökkentése, valamit az időkényszer miatt, kompromisszumos megoldásokat alkalmaznak, amely sok esetben a biztonság redukálásával jár. Erről ugyancsak többet olvashatnak majd az NBSZ NKI „IoT eszközök biztonsági kérdései" jelentésében. Fontos, hogy a számunkra megbízható és magánéletünk szempontjából legfontosabb eszközeinket, mint a számítógépek, mobiltelefonok, tabletek tartsuk a fő hálózaton, minden mást a Vendég vagy Okoseszköz hálózatra rakjuk.



5. ábra Vendéghálózat konfigurációja.

WPS kikapcsolása

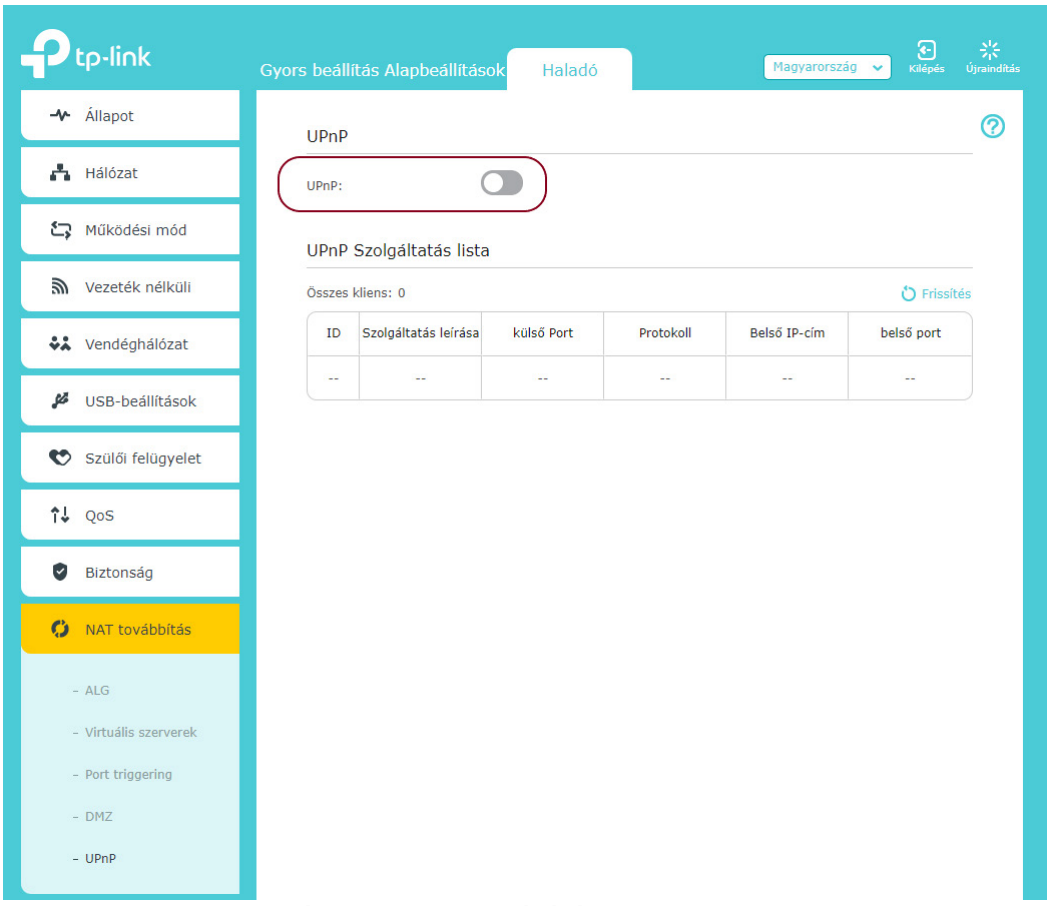
A WPS vagy WiFi Protected Setup funkció képes egy leegyszerűsített folyamattal hozzárendelni eszközöket a vezeték nélküli hálózatunkhoz. Sajnos a kényelem mellékhatása, hogy könnyen kihasználható. A **WPS PIN** egyszerűen akár **percek alatt feltörhető**, ezért annak **kikapcsolása javasolt** a router kezelőfelületén.



6. ábra WPS protokol beállítások.

UPnP kikapcsolása

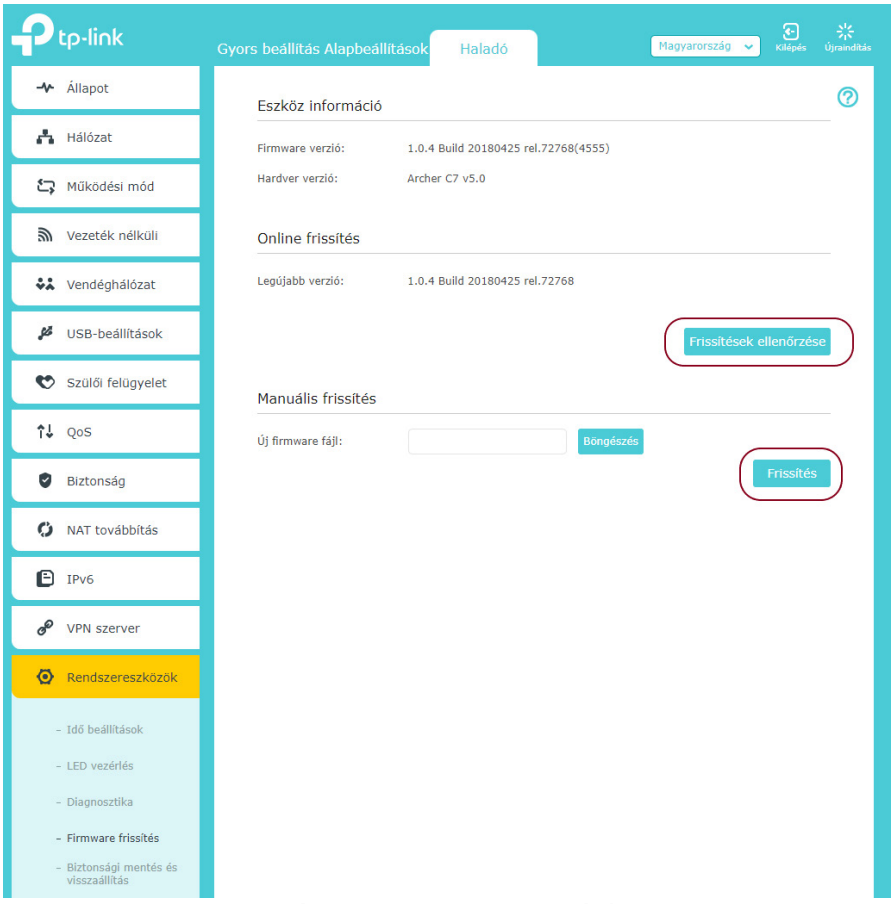
Egy másik funkció, amely arra szolgál, hogy az életünket megkönnyítse az a UPnP avagy Universal Plug and Play. Sok okoseszköz által használt protokoll könnyebb internet kapcsolatot biztosít az eszközeinknek a gyártó szervereivel vagy más felekkel. UPnP-t használó eszköz vagy szoftver képes a routeren portot kinyitni, így kintről is hozzáférhetővé válik a helyi belső hálózatunk. Egy támadó képes saját eszközét egy általunk és a router számára megbízható eszköznek tettetni, amely által szabad utat kap minden ehhez tartozó forgalom. Sok példát látunk erre a DDoS támadásoknál használatos botnet fertőzésekkel kapcsolatban is. Erről itt olvashatnak többet (https://nki.gov.hu/it-biztonsag/tudastar/robothalozat-botnet-2/).



7. ábra UPnP beállítási menüpont.

Frissen tartott firmware

A routerek rendelkeznek egy beágyazott vezérlő szoftverrel (firmware), ami az eszköz működéséért felel. Sajnálatos tény, hogy a felhasználók igen kis százaléka frissíti a routerek firware-jeit, holott ez jelenti a legnagyobb biztonsági kockázatot a rendszereinkben. A firmware hibák és azok pontos kihasználásainak módja sok esetben publikusan elérhetők a nyílt interneten. Amennyiben egy támadó képes adatokat lekérdezni a routerünkről, könnyen meg tudja állapítani milyen sérülékenységen keresztül képes bejutni az otthoni hálózatunkba. Ezért érdemes rendszeresen ellenőrizni, hogy elérhető-e **szoftver frissítés** a routerünkre, ugyanis a gyártó a fejlesztések mellett a biztonsági hibákat is kijavítja. Friss firmware, kevesebb hiba, biztonságosabb hálózat.



8. ábra Frimware frissítés.

NEMZETI
KIBERVÉDELMI INTÉZET

https://nki.gov.hu

titkarsag@nki.gov.hu

+36 (1) 325 7672

Nemzeti Kibervédelmi Intézet

@ nki.gov.hu

Kibertámadás!

2022