CTI Jelentés

IoT eszközök biztonsági kérdései - Az okosotthon

NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NEMZETI KIBERVÉDELMI INTÉZET

Tartalomjegyzék

Bevezetés

Az IoT (Internet of Things, magyarra fordítva: a "dolgok internete") olyan internetre csatlakoztatott eszközök összesége, amelyek képesek kommunikálni más eszközökkel és hálózatokkal, de funkcionalitásuktól függően sokféle feladatra képesek. Sok IoT eszköz az internetkapcsolatot felhasználva teszi lehetővé, hogy a felhasználók távolról is elérhessék és működtethessék az eszközöket, valamint biztosítani tudják a távoli adatbázisokhoz való hozzáférést.

Egyes megközelítések szerint az okostelefonok és a számítógépek is ide tartoznak, azonban van, aki azt vallja, hogy csak azokat az eszközöket lehet az IoT kategóriába sorolni, amelyeknek van IP címe, nem Windows, Linux, Android vagy iOS operációs rendszert futtat, nem igényel közvetlen hozzáférést belső tárolóeszközökhöz és nem tárol személyes adatokat. 2021-ben körülbelül 25 milliárd ilyen eszköz csatlakozott az internetre, és számuk évről évre rendkívüli mértékben növekszik. Egyes becslések szerint 2030-ra elérheti a 75-100 milliárdot is, ami a Föld teljes lakosságára levetítve emberenként 10 ilyen küszéléket fog jelenteni. A piaci és fogyasztói adatokra specializálódott német vállalat, a Statista szerint 2021-ben az IoT eszközök összértéke átlépte a 440 milliárd dollárt és 2030-ba akár az 1000 milliárd dollárt is elérheti. Egyre többen okosítják otthonaikat, egyre több modern egészségügyi központ épül világszerte és egyre több multinacionális vállalat automatizálja a gyártását. Ezekben - és más szektorokban is - egyre nagyobb szerepet kap a mesterséges intelligencia és az internetre csatlakoztatható IoT eszközök. Minden ilyen új berendezés biztonsági kockázatot jelenthet, ugyanis sok esetben a bővülő piaci igények kielégítése, az időnyomás és a profitorientáltság a megfelelő védelem rovására mehet a gyártók részéről. Éppen ezért nagyon fontos, hogy ne csak a mobiltelefonunk és a számítógépünk használata közben legyünk tudatos felhasználók, hanem minden olyan további esetben is amikor egy plusz eszközt csatlakoztatunk az internetre!

Jelen dokumentum célja, hogy bemutassa az olvasó számára a piacon elérhető IoT eszközök sokaságát, ismertesse azok biztonsági hiányosságait és megoldást adjon ezen kockázatok minimalizálására, elkerülésére, hogy az egyre népszerűbb eszközök széleskörű funkcionalitása biztonságosan kihasználható legyen.

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) honlapján elérhető az Otthoni hálózatok biztonsága című CTI tájékoztató, amely bemutatja az otthon kialakítható hálózatok biztonsági kockázatait és olyan módszerek és technikák betartására tesz javaslatot, amelyekkel nagy mértékben csökkenthető hálózataink sérülékenysége, ezáltal az otthoni IoT eszközök támadhatósága is.

Az okosotthon

Mitől lesz okos egy otthon? A válasz egyszerű: a benne található okoseszközöktől. Általánosan akkor beszélhetünk okosotthonról, ha a legnagyobb része vagy teljes egésze WiFi-re (vagy különösen IoT eszközökre optimalizált hálózatokra, például Zigbee-re vagy Z-wave-re) csatlakoztatott készülékekkel van berendezve. Természetesen egy régi építésű házat vagy lakást is átlehet alakítani okosotthonná, ha beszerezzük és telepítjük a hozzá szükséges eszközöket, de az a jellemző, hogy az újonnan épülő ingatlanokat már annak megfelelően tervezik, hogy okosotthonokként funkcionáljanak. Ezek olyan – a fogyasztókra összpontosító – eszközök, amelyek a háztartási funkciók automatizálását segítik és általában valamilyen közös egységben összpontosul a vezérlésük (például okostelefonról irányíthatók). Ezek közül a legnépszerűbbek:

- Otthoni hangvezérlők: ezek olyan vezérlőegységek, amelyek segítségével más okos eszközökkel tudunk interakcióba lépni. Irányíthatjuk a különböző médiaszolgáltatásainkat, ébresztőket, lámpákat vagy termosztátokat. Számos megvalósítása létezik, ilyen például a Jibo, Mycroft, Amazon Echo, Apple Homekit, Ivee Sleek vagy a Google Home Voice Controller.

- Okos ajtócsengők kamerával és okoszárral: a készülék értesítést küld a tulajdonosa számára, ha valaki megnyomta a csengőt. Bárhonnan válaszolhatunk, élőképet kaphatunk a kamera segítségével és az okoszárral akár be is engedhetjük őket. A kamerafelvétel aktiválódhat mozgásérzékelő szenzorok hatására, gombnyomásra vagy akár megállás nélkül is rögzíthet.

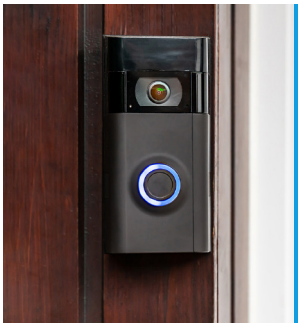
- **Okosvillanykapcsoló:** olyan falra szerelhető villanykapcsolók, amelyeket érintőképernyőn, wifin keresztül a telefonunkon vagy pedig hanggal tudunk vezérelni.
- **Levegő minőség monitor:** olyan eszköz, amely képes valós időben analizálni adott térben a levegő minőségét és visszajelzést ad arról a felhasználónak
- **Okosfüstjelző:** képes érzékelni a füstöt, egyes típusok pedig az emberekre és állatokra rendkívül veszélyes szénmonoxidot is. Hang- és fényjelzést ad, valamint értesítéseket küld a szinkronizált alkalmazáson keresztül a felhasználónak.
- **Okostermosztát:** segítségével könnyedén vezérelhetjük a hűtő-fűtőrendszerünket akár távolról is. Nyomon követhetjük fogyasztásunkat és energiát takaríthatunk meg a használatával.
- **Okosizzók és világításrendszerek:** az alkalmazáson keresztül vagy hangutasításokkal vezérelhető világításrendszer segítségével egyszerűen hozhatunk létre olyan fényt és világítást amire éppen szükségünk van, legyen az olvasófény, hangulatvilágítás vagy akár fokozódóan erősödő fény. Zenékkel és filmekkel is szinkronizálhatjuk.
- **Okoskonnektor:** minden olyan elektronika berendezés, amit ezen keresztül helyezünk áram alá, megkapja azokat az alapfunkciókat amellyel a legtöbb IoT eszköz rendelkezik. Ilyen a távoli vagy hangvezérléses be- és kikapcsolás, távoli felügyelet, valamint szabályokat, ütemezéseket alakíthatunk ki és értesítéseket küldhetünk vele a telefonunkra.

A felsorolt példákból jól látszódik, hogy okoseszközök mindegyike csatlakoztatható valamely hálózatra és egy alkalmazáson keresztül elérhetők és irányíthatók, ezzel megteremtve a kényelmet és biztonságérzetet a felhasználó számára.

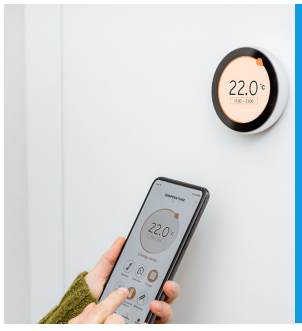
Rengeteg egyéb ilyen készülék létezik még: okostv, okoshűtő, okosporszívó, okoscserép, kamera- és riasztórendszerek, árnyékolástechnikák, öntözésrendszerek, okoshangfalak és hangrendszerek, okostoalett, okosszemetesláda, okosotthon kiberbiztonsági hub stb.

Számuk napról napra nő és egyre komplexebb kialakításokat hoznak létre a gyártók, ezért a velük járó biztonsági kockázat is fokozatosan nő. Minél több eszközünk csatlakozik az internetre, annál nagyobb veszélynek vagyunk kitéve, ugyanis a hackerek vadásszák az olyan eszközöket az interneten, amelyek nincsenek megfelelő biztonsággal ellátva.

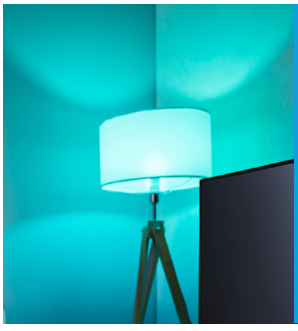

Otthoni hangvezérlő


Okos ajtócsengő


Okos füstjelző



Okos termosztát


Okosizzók, okoslámpák


Okoskonnektor

A biztonság

Aggodalomra adhat okot az IoT eszközök biztonsága, mivel megjelenésük óta meglehetősen vonzó célpontot nyújtanak a kiberbűnözők számára. Általános érvényű, hogy egy gyenge vagy semmilyen védelemmel ellátott okoseszköz sokkal könnyebben (utóbbi esetben minden erőfeszítés nélkül) támadható és állítható a támadó szolgálatába, mint egy tűzfalakkal, vírusvédelemmel és egyéb védelmi rendszerekkel rendelkező számítógép. E támadások többsége egyszerű biztonsági problémákból ered, például az alapértelmezett jelszavak megtartásából egy telnet szolgáltatáson.

A Telnet egy olyan protokoll, amely távoli hozzáférést biztosít egy másik számítógéphez, és akár programokat is futtathat rajta a felhasználó. Mivel a Telnetben nincs semmilyen titkosítás, ezért manapság már ritkán használják. Helyét az SSH (Secure Shell) protokoll vette át, amelyet egy biztonságos csatorna kiépítésére fejlesztettek ki.

Az okosotthon IT biztonsága a legtöbb esetben a routernél és annak konfigurációjánál kezdődik. A korábbiakban felsorolt előnyök kiaknázásához elengedhetetlen, hogy távolról is kommunikálni tudjunk az eszközeinkkel, ebben segít a router. Ha egy támadó feltett szándéka hozzáférést szerezni egy okoseszközhöz vagy betörni az otthoni hálózatunkba, akkor az esetek túlnyomó többségében a hibásan vagy nem megfelelően beállított routernél fogja kezdeni. Ha elvégzünk néhány alapvető módosítást és egyes beállításokra külön odafigyelünk, akkor olyan mértékben megnehezíthetjük a támadók dolgát, hogy a hálózatunk már nem is lesz vonzó célpont számukra.

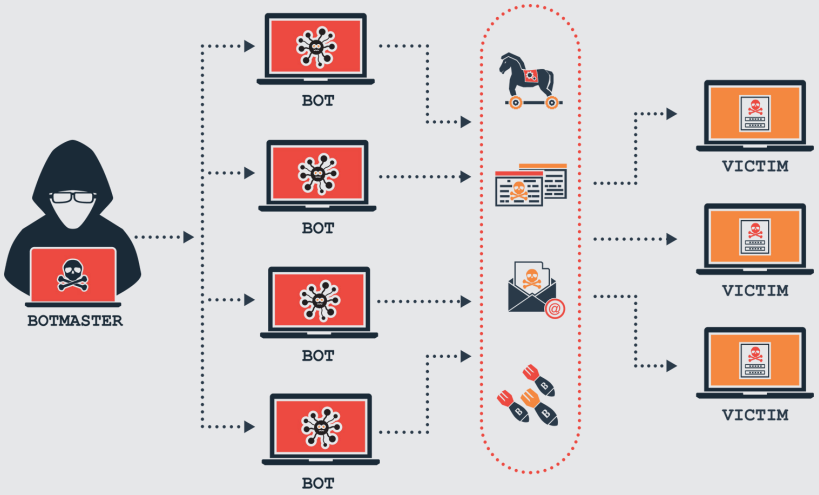
Azonban, ha óvatlanok vagyunk az eszközeink biztonsági beállításaival kapcsolatban, és egy hekker sikeresen be tud törni a hálózatunkba, veszélybe kerülhetnek a személyes adataink, amelyet spamelésre, zsarolásra vagy tovább értékesítésre is felhasználhatnak.

A fizikai fenyegetettség sem elhanyagolandó. Amennyiben a kameráinkhoz vagy olyan szenzorokhoz tud hozzáférést szerezni a hekker, mint az okostermosztát, könnyedén ki tudja figyelni a napi rutinunkat. Ha például reggel 8-kor a kiszemelt áldozat elmegy dolgozni, és akár manuálisan, akár automatikusan lejjebb viszi a maximális hőmérsékletet, majd délután hazaérkezéskor vagy nem sokkal még azelőtt visszaemeli azt, akkor ez egyértelmű indikátor lesz a támadó számára, hogy adott esetben mikor tud zavartalanul betörni az áldozat lakásába. Ezzel kapcsolatos védelmi intézkedésekről a dokumentum végén, az *Az NBSZ-NKI javaslatai a felhasználók számára* című fejezetben olvasható.

Botnetek

Bár elképzelhető, hogy célzott támadás áldozataivá válunk, leggyakoribban mégis egy botnethez próbálják becsatolni a gyenge védelemmel ellátott IoT eszközeinket.

A robothálózat (továbbiakban botnet) egy fertőzött informatikai eszközökből álló hálózat, amelyet a botnet gazdája többféle károkozásra is alkalmazhat. A fertőzött munkaállomások felhasználásának célja főképp kéretlen levelek kiküldése, szenzitív (például banki) adatok eltulajdonítása vagy pedig szolgáltatás megtagadást okozó támadások (Denial of Service - DoS) indítása.



A DoS támadások olyan elektronikus támadások, amelyek rendszereket, szolgáltatásokat vagy hálózatokat képesek olyan mértékben leterhelni, hogy az érintett rendszer szolgáltatása, vagy hálózata elérhetetlenné válhat. Ez egyrészt a rendszerek megbénításával, másrészt a hálózati forgalom növelésével érhető el, amelynek eredménye, hogy a legitim adatforgalom nem éri el a célrendszert. A DoS támadás származhat egyetlen rendszertől, vagy akár rendszerek csoportjától is. Ez utóbbi esetet elosztott szolgáltatás-megtagadással járó (DDoS) támadásnak nevezzük.

DDoS támadások egy másik csoportja, amelyekben bizonyos UDP protokollt használó szolgáltatásokat (NTP, DNS) használnak a célpont túlterhelésére. Ebben az esetben nyíltként konfigurált szervereket szólítanak meg nagyszámú kliensről, forráscímként a túlterhelni kívánt célpont IP címét megadva.

A motivációs célok között megtalálható többek között az anyagi előnyszerzés (pl.: szervezet zsarolása), valamint ideológiai célok is (pl.: tiltakozás egy ország, vagy szervezet ellen), (Anonymous, ISIS).

Az NKI oldalán bővebb információkat olvashat a botnetekről és DDoS támadásokról.

Mirai

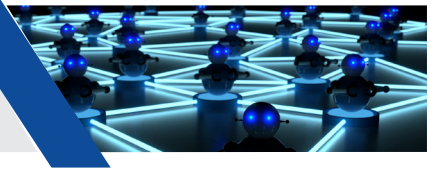
A Mirai botnetet a MalwareMustDie csoport fedezte fel 2016 augusztusában. Először Brian Krebs-nek, annak az újságírónak a blogját vették célba a botnettel, aki egyes információk szerint felfedte egy hekker kilétét. A világtörténelem egyik legnagyobb méretű kibertámadását mérték a blogjára, amely során több mint 600 Gbps-os forgalommal bombázták.

A Mirai botnet igazi ereje 2016 októberében mutatkozott meg, amikor a Dyn nevű DNS-szolgáltatót támadták meg vele. A három hullámban érkező támadás során, olyan amerikai cégek szolgáltatásai váltak teljesen elérhetetlenné, mint a Github, The New York Times, Amazon, Netflix, Reddit, Twitter, CNN. A támadás alatt 1,2 Tbps adatforgalmat mértek és több tíz millió IP címről érkezett. Az akciót követően a Mirai fejlesztői publikussá tették

a forráskódjukat és egy hónappal az incidens után közel 1 millió Deutsche Telekom ügyfélnek szűnt meg az internetszolgáltatása egy Mirai altípus miatt.

Azóta is számos variáns készült, komoly problémát és fejtörést okozva ezzel a kiberbiztonsági szakembereknek.

Gafgyt



A Bashlite (más néven Gafgyt) olyan rosszindulatú szoftver, amely Linux rendszereket fertőz meg DDoS támadások indítása céljából. Eredetileg Bashdoor néven is ismert volt, de ez a kifejezés mára már a rosszindulatú szoftver által használt exploit módszerre utal. 400 Gbps sebességű támadások indítására is használták már. 2016-ra több mint egymillió eszközt fertőzött meg.

VPNFilter

A VPNFilter egy olyan rosszindulatú szoftver, amelyet a routerek és a hálózathoz csatolt tárolóeszközök megfertőzésére hoztak létre. 2018 májusában világszerte körülbelül 500 000 routert fertőzött meg. A kártevő alkalmas adatlopásra, képes kikapcsolni parancsra a fertőzött routert, valamint fennmaradni a kapcsolatot akkor is, ha a felhasználó újraindítja a routert.

Virut

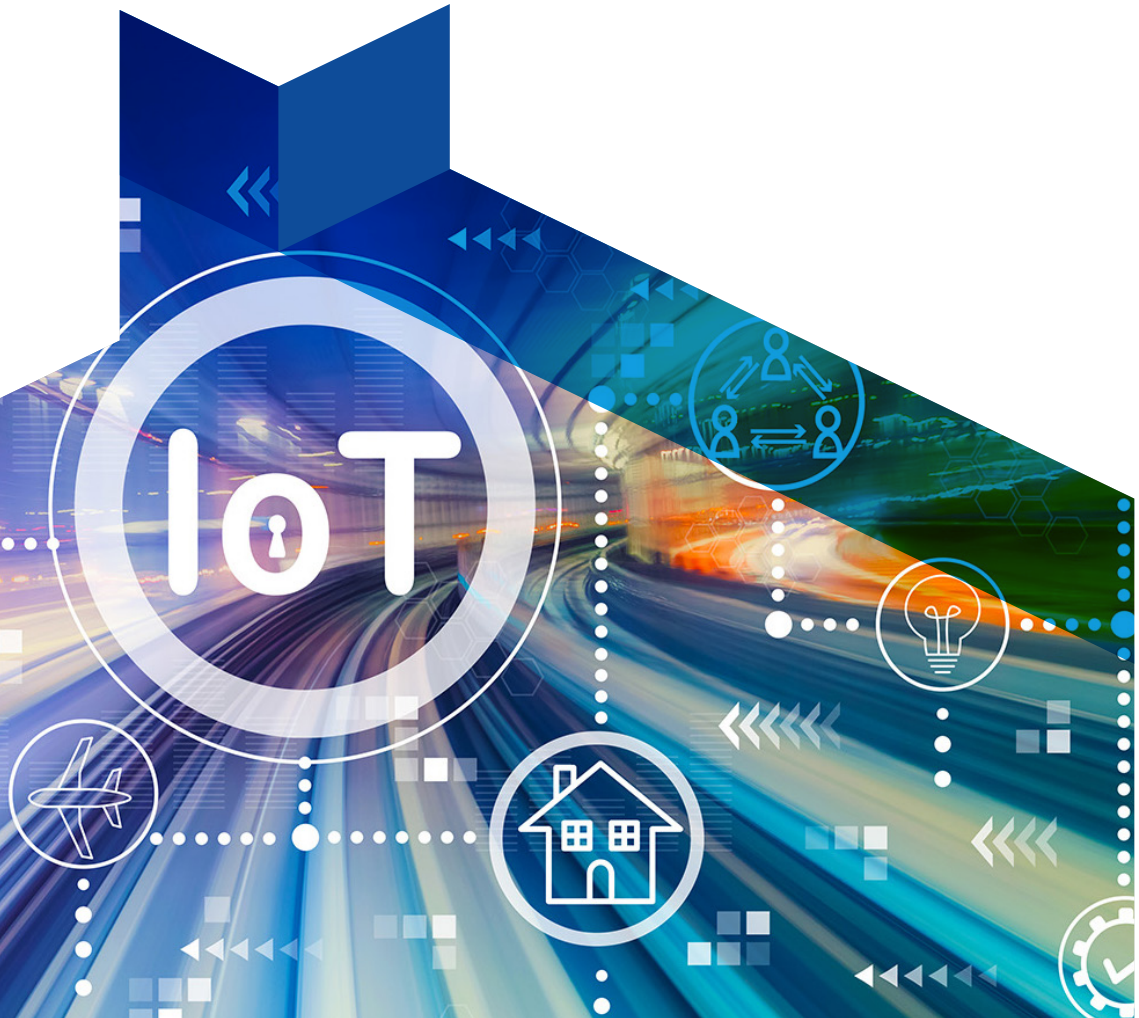
A Virut egy 2006-óta működő malware botnet, az egyik legelterjedtebb fertőzésterjesztő a világhálón. A kártevő a Microsoft Windows rendszerek ismert sebezhetőségeit használja ki. Elsősorban futtatható állományokat fertőz (.EXE, .SCR), de létezik olyan variánsa is, amely ASP, HTML, vagy PHP fájlokat károsít. Férgekhez hasonlóan sokszorosítja magát helyi, eltávolítható (pl. USB), vagy hálózati meghajtókra. Előfordulhat, hogy egy hátsó kaput (backdoor) nyit a fertőzött gépen, ezzel hozzáférést engedve ahhoz a támadónak.

Egyéb kártevők, botnetek

Rengeteg olyan botnet létezett a 2000-es évektől kezdve, amelyeknek a működését sikerült megakadályozni a hatóságoknak. Ilyen volt például a Storm, Mariposa, ZeroAccess, 3ve, Methbot, Kraken, Grum vagy a Cutwail. Vannak azonban a mai napig is aktív botnetnek, mint például a fent említett Mirai, vagy a Zeus, Dridex és Emotet.

Összefoglalás

Az okosotthon, így a benne foglalt okoseszközök minket, a kényelmünket és a jövőnket szolgálják. Számuk és a bennük rejlő lehetőségek folyamatosan nőnek és bővülnek. Ez a tendencia ráadásul egyre csak gyorsulni fog az idő előrehaladtával, elképzelhető, hogy néhány évtizeden belül minden háztartás az ilyen és a majdani fejlettebb technológiák mentén fognak felépülni és üzemelni. Éppen ezért rendkívül fontos, hogy a minket szolgáló gépeket, műszereket és eszközöket a lehető legbiztonságosabban használjuk, hogy magunkat és szeretteinket, valamint anyagi javainkat biztonságban tudhassuk. Használjuk ki az IoT adta lehetőségeket, de olyan módon, hogy hasznunkra váljanak, ne pedig a kárunkra.



Az NBSZ-NKI javaslatai felhasználók számára

IoT eszközök üzembehelyezésnél, okosotthon kiépítésénél érdemes az alábbi szempontokat figyelembe venni:

- Nevezzük el úgy a hálózatunkat, hogy az hozzánk ne legyen köthető!
- Tegyük rejtetté a hálózatunkat (SSID)!
- Állítsunk be WPA2-PSK (AES) titkosítást a routerünkön!
- Hozzunk létre külön vendéghálózatot! A legbiztonságosabb módszer, ha külön VLAN-t hozunk létre az eszközeinknek.
- A routerünk beüzemelése után azonnal változtassuk meg a felhasználónév/jelszó párost! Alapértelmezetten a legtöbb router az admin, root, system, user, pass, password és egyszerű, rövid számsorok kombinációit használják. Ez egy hekker számára olyan, mintha bezárnánk az ajtónkat kívülről, de benne hagynánk a kulcsot.
- Vizsgáljuk át minden beüzemelt IoT eszköz alapbeállításait és szükség esetén módosítsunk azokon! Amelyeknél lehetséges, állítsunk be jelszót vagy pin kódot!
- Ha van elérhető új firmware, azonnal töltsük le, mivel sok esetben ezeknek a frissítéseknek az eszköz biztonságosabbá tétele a szerepük! Telepítés után böngésszük át újra a beállításokat, mert elképzelhető, hogy egyes beállítások a frissítés következtében módosultak!

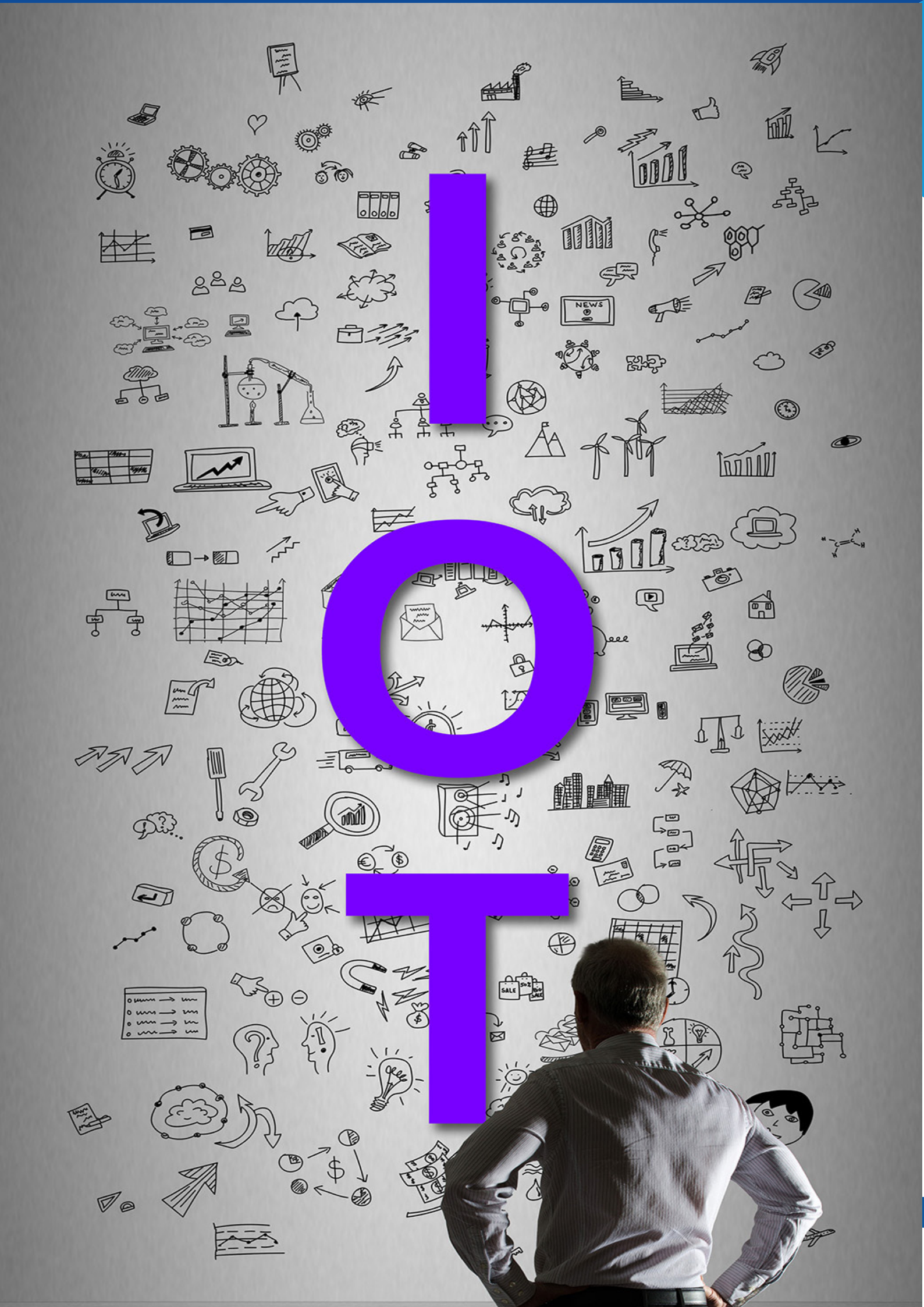
- Mobileszközeinkkel mindig kerüljük el a nyilvános wifi hálózatokat, használjunk helyettük mobil internetet!
- Lehetőség szerint használjunk VPN szolgáltatást!
- A későbbi fertőzések elkerülése érdekében használjunk naprakész vírusirtót, tűzfalat, valamint rendszeresen végezzünk fájlrendszer ellenőrzést!
- Kapcsoljuk ki az Universal Plug and Play funkciót (UPnP) a router beállításai között!

A jelszavak választásánál érdemes az alábbi szempontokat figyelembe venni:

- Ne legyen ránk jellemző, mert kevés információ birtokában is könnyen kitalálható (pl.: családtag neve + születési dátum egy rövid kereséssel a közösségi oldalakon kideríthető).
- Nem szerencsés, ha a jelszó csak egy szóból áll (például az „almafa" szó biztosan szerepel egy támadó által kipróbálandó jelszavak listájában).
- Jó, ha a jelszó hosszú és többféle karaktert (kisbetű, nagybetű, szám, írásjel) tartalmaz, mert ezzel megnehezíti a brute force technikával való feltörést.
- A legjobb, ha néhány szóból álló jelmondatot választunk, amelyben van kisbetű, nagybetű, szám és írásjel is. Ezt könnyű megjegyezni, azonban nehéz kitalálni, brute force technikával feltörni pedig szinte lehetetlen.

A jelszavak kezelése történjen az alábbiak szerint:

- Fontos, hogy ne adjuk „kölcsön" a jelszavunkat, hiszen nem tudhatjuk, hogy az adott személy körültekintően fogja-e kezelni.
- Ne írjuk fel a jelszavunkat, mert ez könnyen illetéktelen kezekbe kerülhet!
- Ne használjuk mindenhol ugyanazt a jelszót, ha a támadók egyet feltörnek, minden más rendszerünkhöz hozzáférhetnek!
- Rendszeresen változtassuk meg a jelszavainkat, a támadónak minél több ideje van próbálkozni, annál nagyobb valószínűséggel tudja megszerezni a hozzáférésünket!
- Használjunk valamilyen jelszókezelő rendszert! Ezek olyan szoftverek, amelyek titkosított formában tárolják jelszavainkat, így azokhoz illetéktelenek (ideális esetben) nem – vagy csak irreálisan nagy erőforrás ráfordításával – férhetnek hozzá. A megoldás előnye, hogy ehhez csupán egyetlen, ún. mesterjelszót kell fejben tartanunk, azt, amellyel hozzáférhetünk magához a jelszószéfhez. A mesterjelszóból kerül leképezésre az a titkosító kulcs, amivel a hitelesítő adatokat (felhasználónév, jelszó) tároló adatbázis – esetlegesen további kriptográfiai komponensek bevonásával – titkosításra kerül (1Password, KeePass, Dashlane, RoboForm, LastPass, Password Safe, Bitwarden, Keeper, Kaspersky Password Manager, LogMeOnce stb.).


IoT
NEWS
SALE

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

titkarsag@nki.gov.hu

+36 (1) 325 7672

Nemzeti Kibervédelmi Intézet

@ nki.gov.hu

Kibertámadás!
podcast

2022