TLP: WHITE
Szabadon terjeszthető!

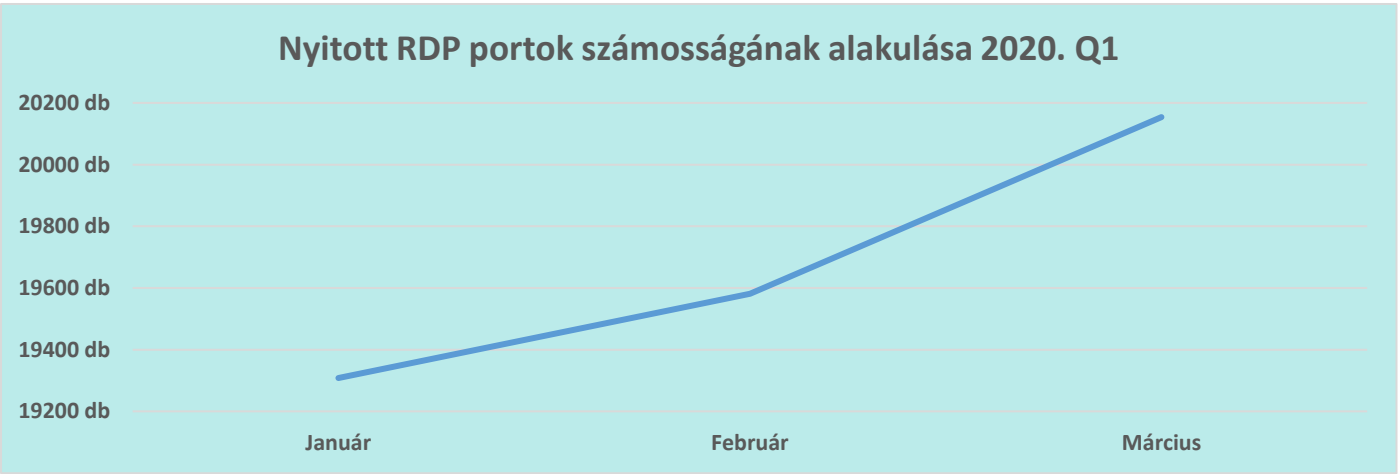
Riasztás
Nyitott RDP port biztonsági kockázatai
(2020. április 06.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) **riasztást** ad ki **nyitott RDP port biztonsági kockázatai** témában. Az NBSZ NKI tapasztalatai alapján az elmúlt közel másfél év során jelentősen megnövekedett az olyan informatikai biztonsági incidensek száma, amely során az ismeretlen támadók a nem megfelelően konfigurált RDP szolgáltatást kihasználva, azon keresztül zsarolóvírust juttattak a támadott rendszerbe. A támadások során a ransomware fertőzésnek köszönhetően jellemzően az intézmény adatainak és szervereinek jelentős része, egyes esetekben az egésze titkosításra került, ez által megbénítva az adott szervezet működését. A hazai és nemzetközi partnerektől származó információk alapján az ilyen típusú támadások segítségével terjesztett zsarolóvírusok elsődleges célpontjai piaci vállalatok és állami szervezetek.

Remote Desktop Protocol (RDP): a Microsoft által fejlesztett protokoll, amely grafikus felületet biztosít a felhasználók és adminisztrátorok számára, hogy hálózati kapcsolaton keresztül csatlakozzanak egy másik számítógéphez. Alapértelmezetten a TCP3389 porton üzemel.

A 2020-as év első negyedévében az internet irányából szabadon elérhető RDP portok (TCP3389) számossága a korábbi tendenciához képest látványos emelkedést mutat. A március hónapban az emelkedés mértéke közel 110% a január és februári adatokhoz képest. Az emelkedés egyik oka lehet, hogy egyre több szervezet biztosítja munkavállalói számára az otthoni munkavégzés lehetőségét, amelyet – a bevezetési határidők szűkössége miatt – nem minden esetben sikerült kellően biztonságosan beállítani.



A nem megfelelően konfigurált RDP elérés így olyan biztonsági kockázatokat hordozhat magában, amelyek adott esetben a szervezet teljes működését megbéníthatják, ellehetetlenítve ez által a napi szintű feladatok ellátását.

A támadások sikerességének csökkentése érdekében, kiemelt tekintettel a távoli asztali elérést biztosító szolgáltatásokra, az NBSZ NKI az alábbi kockázatcsökkentő / megelőző intézkedések mihamarabbi megtételét javasolja:

- **Az RDP kiszolgáló** beállítása, hogy **publikus IP címekről tiltva legyen a TCP3389 port elérése.**
- Amennyiben mégis szükséges **RDP** elérés, a **hozzáférés korlátozása** megadott **IP címekre**.
- **Üzemeltetéshez használt portok** (SSH, RDP, Telnet, LDAP, NTP, SMB, stb.) **külső hálózatból történő elérésének tiltása**, üzemeltetési feladatok ellátásához javasolt a rendszerek VPN (többfaktoros azonosítással) kapcsolaton keresztül történő elérése.
- **Az RDP elérés dedikált gépről történjen, ne a felhasználó otthoni gépéről.**
- **RDP** hozzáférés és hozzáférési kísérletek **full verbose naplózása** (nem csak bejelentkezés, hanem minden tevékenység, pl. fájlelérés). Naplók mentése, nem ciklikus felülírása.
- **A legkisebb jogosultsági elv** (least privilige) **alkalmazása**, ha nem szükséges ne legyen admin jogköre a távoli felhasználónak.
- **Bejelentkezések** rendszeres **felülvizsgálata** a naplóállományok alapján.
- Felhasználói **fiókok zárolására vonatkozó házirend kialakítása.**
- **Jelszavak kötelező periodikus cseréje, szigorú jelszóházirend alkalmazása mellett.**
- **Megfelelő biztonsági mentési és visszaállítási stratégia kidolgozása.**
- **Katasztrófa utáni helyreállítási terv kidolgozása** (DRP).
- Amennyiben lehetséges, **többfaktoros azonosítás** engedélyezése **az RDP bejelentkezéshez.**
- A **nyitott portok alapértelmezett értékeinek megváltoztatása** (security by obscurity) megnehezíti az automatákkal végzett letapogatást, így a szolgáltatás támadásokkal szembeni kitettsége is csökkenthető.
- **Nyitott portok felülvizsgálata,** a szükségtelen portok bezárása, a szükséges portok fokozott felügyelete.
- A **gyakran használt portok** internet irányából történő **elérésének korlátozása** (megadott IP címekről, bizonyos felhasználók számára).
- **Határvédelmi rendszerek szoftvereinek naprakészen tartása.**
- **Alkalmazások és operációs rendszerek naprakészen tartása.**
- **Határvédelmi eszközök feketelistájának frissítése** (több gyártó rendelkezik nyilvánosan elérhető listákkal pl.: Cisco), ezáltal csökkentve a támadás kockázatát.
- A **szükségtelen felhasználói fiókok felfüggesztése**, a távoli eléréssel rendelkező felhasználók szükséges mértékre történő csökkentése, **felhasználók jogosultságainak időszakos felülvizsgálata**.
- Rendszeres online és **offline** (szalagos egység, külső merevlemez) **biztonsági mentés**, archiválás.

A fentiekben megfogalmazott javaslatok végrehajtása minden olyan zsarolóvírus esetében jelentősen csökkentik a biztonsági esemény bekövetkeztét, amelyeket RDP segítségével juttatnak a támadók a rendszerbe.

Biztonsági incidens bekövetkezése esetén az NBSZ NKI az alábbiakat javasolja:

- Sikeres támadás esetén az érintett eszköz **hálózatról** történő **leválasztás**át.
- Ransomware fertőzés esetén az érintett adathordozók helyreállítása előtt **bitazonos másolat készítését.**
- **Incidens bejelentését** az NBSZ NKI részére a CSIRT@nki.gov.hu e-mail címen, vagy az nki.gov.hu weboldal incidensbejelentő felültén keresztül.
  - **A bejelentés tartalmazza az incidenssel kapcsolatos alapvető információkat:**
    - A biztonsági esemény leírása (károkozás mértéke, mely kliens és szervertartalmak sérültek).
    - Esemény bekövetkeztének és észlelésének időpontja.
    - Hogyan következhetett be a biztonsági esemény?
    - Milyen intézkedések történtek?
    - Ransomware fertőzés esetén a „ransom note”, valamint 2 db titkosított állomány, fájlkiterjesztés.

További hivatkozások:

- https://nki.gov.hu/it-biztonsag/hirek/ezek-az-rdp-brute-force-tamadasok-fobb-jellemzoi-a-microsoft-szerint/
- https://nki.gov.hu/it-biztonsag/hirek/ujabb-windows-tavoli-asztal-sebezhetosegre-derult-feny/
- https://nki.gov.hu/it-biztonsag/hirek/ujabb-veszely-leselkedik-a-tavoli-asztallal-elerheto-felhasznaloi-fiokokra/
- https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-phobos-zsarolovirus-terjedeserol/
- Közigazgatási Kibervédelmi Eszköztár
- Levélfejléc kinyerése
- Zsarolóvírusok
- Adathalászat
- Adatbiztonság a munkahelyen
- Biztonságos internethasználat
- Megszemélyesítéses támadások
- Pszichológiai befolyásolás
- Biztonsági mentés

Nemzetbiztonsági Szakszolgálat
Nemzeti Kibervédelmi Intézet
Telefon: +36-1-336-4833
Fax: +36-1-336-4886
Incidensbejelentés: csirt@nki.gov.hu