TLP:CLEAR
Szabadon terjeszthető!

Riasztás ipari vezérlőrendszereket érintő kampányról

Tisztelt Ügyfelünk!

A **Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet** (NBSZ NKI) riasztást ad ki egy **kritikus infrastruktúrákat célzó, jelenleg is aktív** támadási kampány kapcsán. A rendelkezésre álló elemzés szerint a kampány során iráni kötődésű szereplők **ipari vezérlőrendszerekhez**, ezen belül Rockwell Automation / Allen-Bradley PLC-khez fértek hozzá, és azok manipulálásával **működési zavarokat idéztek elő**.

A támadások sajátossága, hogy nem kifinomult technikai sérülékenységekre épülnek, hanem elsősorban a rendszerek **nem megfelelő elérhetőségét és a hiányos hozzáférés-kezelését** használják ki. Ez azért jelent különös kockázatot, mert ebben az esetben **a hagyományos védelmi intézkedések**, így önmagukban a rendszeres frissítések vagy a vírusvédelmi megoldások **nem feltétlenül elegendők** a fenyegetés érdemi csökkentésére.

A támadók olyan ipari környezeteket céloznak, amelyek **közvetlen hatással vannak fizikai folyamatokra**, így például az energiaellátásra, a vízkezelésre vagy a gyártási működésre. Ezek a rendszerek eredetileg nem nyilvános hálózati működésre készültek, ugyanakkor a digitalizációs és távoli üzemeltetési igények következtében sok esetben részben vagy teljes mértékben internet felől is elérhetővé váltak. A támadók **gyakran legitim eszközöket és gyártói szoftvereket használnak**, valamint **valós vagy megszerzett jogosultságokkal dolgoznak**, ami megnehezíti az észlelést és a védekezést.

Az érintett termékek a Rockwell Automation / Allen-Bradley PLC-k, ugyanakkor potenciális célpontot jelenthetnek más gyártók PLC megoldásai is.

Javasolt intézkedések

Javasolt a PLC-k közvetlen **internetes elérhetőségének megszüntetése**, és az ipari vezérlőrendszerek kizárólag **megfelelően szabályozott**, biztonságos átjárón, valamint tűzfalon keresztüli **elérésének biztosítása**. Indokolt továbbá annak haladéktalan felmérése, hogy mely OT rendszerek és kapcsolódó menedzsmentfelületek érhetők el külső hálózatokból, és ezekhez milyen jogosultságokkal lehet hozzáférni. Rockwell Automation eszközök esetén javasolt a vezérlő fizikai módválasztó kapcsolóját „run” üzemi állásba helyezni.

IoC-k

IP-cím	IP-cím
185.82.73.165	185.82.73.170
135.136.1.133	185.82.73.164
185.82.73.167	185.82.73.162
185.82.73.168	185.82.73.171

A kapcsolódó IoC-k JSON és XML formátumban elérhetőek a CISA weboldalán.

Nemzetbiztonsági Szakszolgálat
Nemzeti Kiberbiztonsági Intézet
Telefon: +36-1-336-4833