Csak elavult vakhit az internet nélküli számítógépek biztonsága

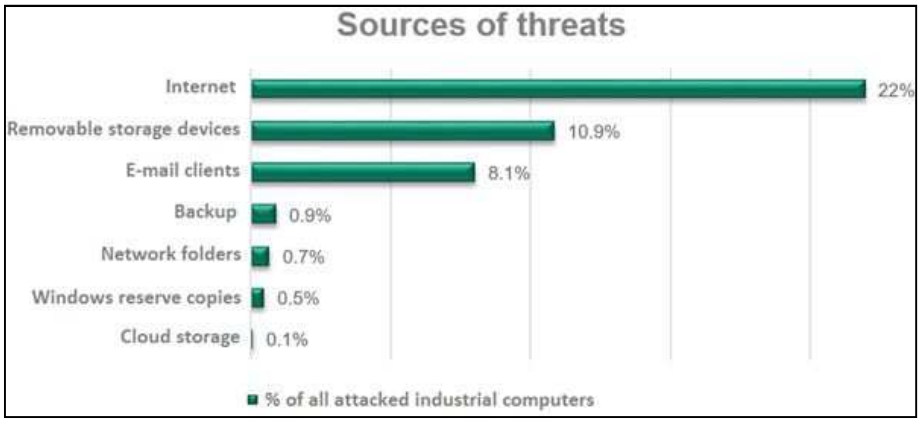
A hálózati rések kihasználásával a támadók képesek megsemmisíteni az ipari nagyvállalatok gyártási műveleteit, ami technológiai katasztrófához vezethet.

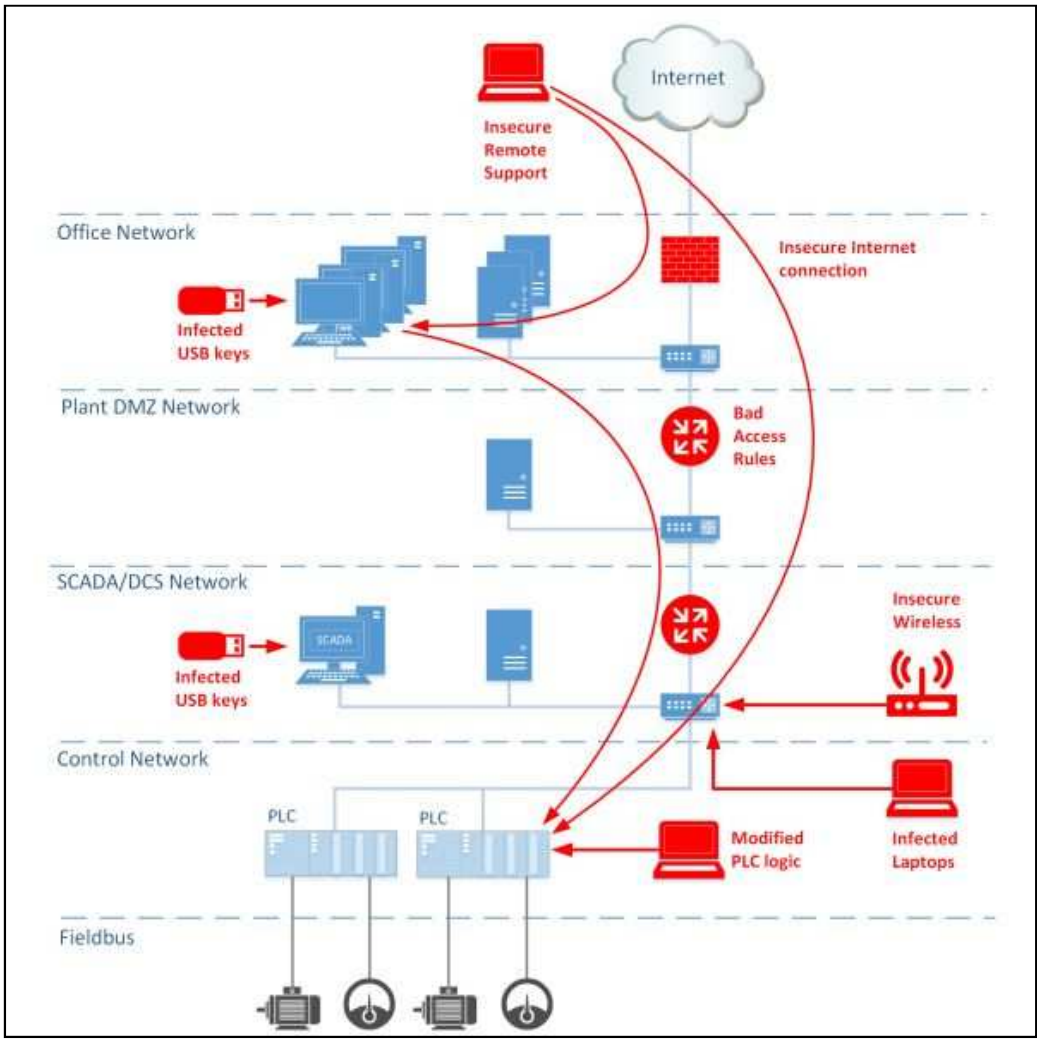
A *Kaspersky Lab* szerint tavaly a technológiai szektor nagyvállalati számítógépeinek 40%-át érte kibertámadás csak a második félévben. A megtámadott számítógépek százalékos aránya a júliusi 17%-ról decemberre már 24%-ra nőtt. A támadások legfőbb forrásai az internet, a mobil adattároló készülékek, valamint rosszindulatú e-mailek és beágyazott forráskódok.

Mivel az ipari vállalatok technológiája és a hálózati rendszere egyre nagyobb mértékben integrált, ezért egyre több kiberbűnöző tekint rájuk potenciális célpontként. A hálózati vagy szoftveres rések kihasználásával a támadók képesek ellopni a gyártási folyamattal kapcsolatos információkat vagy akár megsemmisíteni a gyártási műveleteket, ami technológiai katasztrófához vezethet. A Kasperksy Lab annak érdekében, hogy kiderítse, mennyire elterjedt problémáról van szó, a cég ICS CERT szakembereinek közreműködésével végeztek el célzott kutatásokat. Eredményeik szerint tavaly a második félévben a kártékonyprogram-letöltést és a hozzáférést adathalász weboldalakhoz a vizsgált számítógépek 22%-án blokkolták, ami azt jelenti, hogy majdnem minden ötödik készülék legalább egyszer találkozott fertőzött forrással.

A mérnökök és az üzemeltetők asztali számítógépeinek, amelyek közvetlenül az ICS (Industrial Control System) rendszerében dolgoznak, általában nincs közvetlen internetelérésük a technológiai hálózatok korlátai miatt. Vannak azonban más felhasználók, akiknek egyidejű hozzáférésük van az ICS-hez és az internethez. A Kaspersky Lab kutatása szerint ezek a számítógépek – feltehetően rendszeradminisztrátorok, hálózati rendszergazdák, ipari automatizálási rendszerek fejlesztői és integrátorai valamint alvállalkozók – szabadon csatlakoznak az internetre, mivel nem kötődnek csak egyetlenegy ipari hálózathoz.

Ugyanakkor az internet nem az egyetlen dolog, ami veszélyezteti a számítógépes biztonságot az ICS rendszerekben. A kutatás időszakában a vizsgált számítógépek 10,9%-a jelzett kártékony programot, amint egy mobil adattároló eszközt csatlakoztattak. Az ipari számítógépek 8,1%-a blokkolt már e-mailen keresztül érkező rosszindulatú programot. A legtöbb esetben a támadók adathalász e-maileket használnak, hogy eltereljék a felhasználó figyelmét, és a leggyakrabban olyan dokumentumnak álcázzák a rosszindulatú fájlokat, mint például MS Office- vagy PDF-fájlok. A különböző technikák alkalmazásával a bűnözők gondoskodnak arról, hogy az emberek mindenképp letöltsék a kártékony programot az ipari szervezetek számítógépeire.





A kártékony programok világszerte komoly veszélyt jelentenek az ipari vállalatok számára, hiszen teljesen megbéníthatják a hálózat feletti kontrollt vagy felhasználhatók célzott támadásokra, mert a hálózatban rejlő funkciók rengeteg lehetőséget adnak a kiberbűnözőknek is. „Elemzésünk azt mutatja, hogy a vakhit az internettől izolált hálózati technológiák felé manapság már elavult. A kritikus infrastruktúrák elleni támadások számának növekedése azt jelzi, hogy az ICS hálózatokat megfelelően kell védeni mind a belülről – mind a kívülről érkező rosszindulatú programoktól. Azt is fontos megjegyezni, hogy megfigyeléseink szerint a támadások szinte mindig a leggyengébb láncszemnél kezdőnek, ami nem más, mint az ember.” – mondta *Evgeny Goncharov*, a Kaspersky Lab „Critical Infrastructure Defense” részleg vezetője.

Forrás: https://sg.hu/cikkek/it-tech/124559/csak-elavult-vakhit-az-internet-nelkuli-szamitogepek-biztonsaga

Válogatta: Berke Barnabásné