Föråldrade IT-system inom energi, vatten och transport utan tillräckliga kontroller av IT-säkerheten kräver samordnad kapacitetstestning på EU-nivå, säger EU:s cybermyndighet ENISA

I dag publicerar EU:s IT-säkerhetsmyndighet ENISA en ny rapport med råd för hur kapacitetstestning av industriella styrsystem (Industrial Control Systems-ICS), som ofta är föråldrade, ska kunna samordnas för europeiska industrier. Bland nyckelrekommendationerna är att testning av ICS berör alla EU-länder och att detta skulle kunna hanteras på EU-nivå.

Numera används IT i stor utsträckning av de flesta industriella kontrollsystem; för energi, vatten, transporter m.m. (t.ex. SCADA). Detta är för att förbättra effektiviteten, uppnå kostnadsbesparingar, samt automatisering av olika industriprocesser. Tyvärr medför detta ofta samtidigt dålig planering, otillräcklig information, felaktiga säkerhetskonfigurationer, inkorporering av välkända sårbarheter, samt av nya, oupptäckta eller ännu inte åtgärdade (”patchade”) s.k. ”zero-day”-sårbarheter i ICS/SCADA-system.

Industriella kontrollsystem (ICS) kan ha en livslängd på över 20 år. Därför har de traditionellt utformats som självständiga system, utan tillräckliga säkerhetskrav. Följaktligen är de inte förberedda att ta itu med aktuella hot. För att övervinna dagens säkerhetsluckor krävs en fullständig förståelse av IT-säkerheten (dvs sårbarheter, deras ursprung, frekvens, m.m.) Detta kräver speciella verktyg och metoder för en ordentlig säkerhetsbedömning. Myndigheten understryker därför att det finns ett starkt behov av en särskild strategi för att definiera målen, uppdraget samt en vision för samordning av ICS-kapacitetstestning inom EU.

Denna rapport fokuserar på hur EU:s åtgärder kan samordnas för att nå en gemensam nivå av harmoniserad, oberoende och tillförlitlig ICS-kapacitetstestning, som tar tillvara på redan pågående initiativ inom detta område. Rapporten är baserad på litteraturforskning, en online- enkät samt djupintervjuer med 27 experter från EU, USA, Japan, Indien och Brasilien.

Huvudobservationer samt rekommendationer

Denna studie har resulterat i 36 huvudobservationer samt sju rekommendationer till den offentliga och privata sektorn, med särskild inriktning på EU:s organ:

1: Samordning av kapacitetstestning under offentligt europeiskt ledarskap och med ett starkt stöd från målgruppen; dvs nationella myndigheter och den privata sektorn i EU.
2: Inrättande av en pålitlig och funktionell styrelse med ett tydligt ledarskap
3: Skapandet eller medverkan av specifika arbetsgrupper
4: Utarbetandet av en ekonomisk modell som är anpassad till den europeiska situationen
5: Att genomföra en förstudie för att se hur testningen ska kunna utföras.
6: Upprätta samarbetsavtal med andra organisationer som arbetar med ICS-säkerhet
7: Upprätta “knowledge management” program för ICS-testning

Den verkställande direktören för ENISA, professor Udo Helmbrecht konstaterade: "Det finns ett uppenbart behov av att öka säkerheten i kritisk informationsinfrastruktur och i industriella kontrollsystem eftersom att riskerna ökar; där synnerligen kunniga angripare och naturkatastrofer har visat på svagheterna i systemen. Alla berörda offentliga och privata aktörer uppmanas därför starkt till att ta itu med dessa säkerhetsfrågor på allvar."

Hela rapporten

Bakgrund: EU:s cybersäkerhetsstrategi

För intervjuer: Ulf Bergström, kommunikationschef och talesman, ulf.bergstrom@enisa.europa.eu, mobil: + 30 6948 460 143, eller Adrian Pauna, Expert, resilience@enisa.europa.eu