SecuriOT

DE 10 BUD - INDENFOR ICS-SECURITY

Produktionsvirksomheder står overfor en ny tid. Der tænkes nye veje om integrationen imellem produktionssystemer, forretningsstrategier og de muligheder, som åbner sig i forhold til Industri 4.0.

Sikkerhed i ICS-systemer skal følge med denne udvikling, og derfor har SecuriOT formuleret De 10 Bud, som produktionsvirksomheder bør fokusere på:

1. SKAB OVERBLIK OVER KOMPONENTER OG FORBINDELSER

For at kunne opdage og identificere et evt. cyber angreb, så kræver det et samlet overblik over aktive enheder og forbindelser til og fra produktionsmiljøet.

2. SKAB VISIBILITET

Ændringer i produktionssystemer sker løbende, og nogle af dem kan medføre sikkerhedsbrud. Ved at etablere overvågning af OT/ICS-miljøet skabes visibilitet, som kan opdage unormal trafik. Dette kan evalueres - inden skaden sker.

3. ERKEND CYBER-TRUSLEN

Produktionsmiljøer er ikke isolerede. Angrebene ses på ugentlig basis. Der findes løbende sårbarheder i produktionsenheder, som bruges i produktionen, og som potentielt kan udnyttes af malware eller hackere.

4. UDFØR LØBENDE RISIKOVURDERINGER

Produktionssystemet er kritisk for virksomhedens evne til at tjene penge. Cyber-truslen kan ødelægge det. Løbende vurderinger ift. virksomhedens setup og risikoprofil skal gennemføres, så nødvendige mitigerende aktiviteter kan foretages.

5. SKAB "ALIGNMENT" OG FORANKRING IMELLEM FORRETNINGEN OG SIKKERHEDSSTRATEGIEN

Nye forretningsstrategier og innovative løsninger kan forbedre indtjeningen, men det bør koordineres med sikkerhedsstrategien. F.eks. stiller indførelse af "Industri 4.0 Værktøjer" krav til nye metoder og forretningsmodeller, som vil have indflydelse på sikkerhedsstrategien.

6. OPBYG CYBER-BEREDSKAB OG BACKUP PROCESSER

Når hændelsen sker, så skal beredskabet være klar ift. ansvarsfordeling, procedurer og bemyndigelse, så produktionssystemet hurtigt kan komme tilbage til "betroet tilstand".

7. SKAB EN PROCES FOR HÅNDTERING AF SÅRBARHEDER

Løbende kommer der informationer om sårbarheder i produktionssystemer. Disse kan potentielt udnyttes af malware og hackere. En løbende evaluering af relevante sårbarheder vil minimere risikoen for at blive ramt af cyber-angreb.

8. SKAB EN PROCES FOR STYRING AF ADGANGE OG RETTIGHEDER

Remote adgang til produktionsanlæg til f.eks. vedligeholdelse fra 3. part skal forankres og sikres, så der er styr på adgang og rettigheder til produktionssystemet.

9. ARBEJD MED NETVÆRKSSEGMENTERING

Segmentering af netværk gør det muligt at isolere en evt. spredning af malware. Løbende vedligeholdelse af access-lister og firewall regler vil forbedre sikkerheden i produktionssystemet.

10. SKAB "AWARENESS" I ORGANISATIONEN

Den menneskelige faktor er afgørende. Løbende uddannelse skaber forståelse for mulige konsekvenser af adfærd, som kan kompromittere sikkerheden i produktionsmiljøet.

SECURIOT APS | AGRO FOOD PARK 13 | 8200 AARHUS N | +45 70 27 66 88
WWW.SECURIOT.DK | KONTAKT@SECURIOT.DK | WWW.LINKEDIN.COM/COMPANY/SECURIOTDK