Tema – INDUSTRI 4.0

Säkerhetsutmaningar med Industri 4.0

Fotocred: shutterstock.com

Den allt högre graden av automation och digitalisering ger många fördelar för industrin, men samtidigt öppnar det upp för risker med cyberattacker i de ofta alltför sårbara systemen.

Martin Björnsson. Fotocred: Advenica

Martin Björnsson, Cybersäkerhetsspecialist på Advenica AB som jobbar med informationssäkerhetsfrågor i en digitaliserad värld, konstaterar att risken för sårbarheter ökar ju smartare och mer uppkopplade komponenterna blir.

– För att undvika risken för cyberattacker måste industrier och företag som börjar arbeta med Internet of Things inom industrin, Industrial Internet of Things- IIoT, ha med och prioritera säkerhetsaspekten. Det är viktigt att tänka efter före, att redan då man planerar inköp av nya smarta komponenter även tänka säkerhet. Att ta hand om säkerhetsaspekter i efterhand riskerar att bli en dyr suboptimering, konstaterar han.

Smartare system mer sårbara

Strävan mot Industri 4.0, där IIoT är en del, innebär en önskan att fler och fler system ska kunna tala med varandra och därmed göra processerna mer effektiva.

– Men det innebär också att de smarta komponenterna kommer närmare och närmare den fysiska processen, vilket gör den processen alltmer sårbar. En cyberattack mot produktionssystemen orsakar problem och stora kostnader som ett genomtänkt säkerhetsarbete skulle kunna förebygga.

Ett exempel på ny typ av säkerhetsrisk är att många smarta styr- och reglersystem nu använder vanliga operativsystem som Windows och Linux som behöver uppdateras med jämna mellanrum för att fungera optimalt och för att täppa till de sårbarheter som hittas.

– Men i en miljö där systemens tillgänglighet är a och o är man försiktig med att uppdatera eller göra några förändringar över huvud taget. Det har kommit rapporter om attacker där skadlig kod har installerats i uppdateringar och orsakat stor skada. Dessvärre har det skapat en viss allmän rädsla för att göra även de uppdateringar som är nödvändiga. Men att inte uppdatera sina system och applikationer innebär en säkerhetsrisk i sig självt eftersom systemen blir föråldrade, man upptäcker hela tiden nya luckor som behöver täppas till, förklarar Martin Björnsson.

Finns säkrare sätt att jobba

Det stora it-säkerhetsföretaget Solarwinds blev under 2020 utsatta för ett angrepp där attackerare installerade skadlig kod i företagets uppdatering för övervakningsapplikationen Orion. Detta i sin tur ledde till att den skadliga koden installerades hos Solarwinds kunder när de installerade uppdateringen.

– Attacken drabbade därmed inte endast Solarwinds, utan alla deras kunder som laddade ner uppdateringen. Även de som på något sätt var beroende av en tjänst baserad på Solarwinds produkt drabbades och i Sverige resulterade bland annat detta i att 300 Coop-butiker under ett antal dagar inte kunde ta betalt från sina kunder. Vi behöver lära oss av detta och ta säkerhetsarbetet till nästa nivå.

Vill man skydda sig mot informationsläckage kan uppdateringen göras på ett säkert sätt genom att använda en datadiod som säkerställer enkelriktad kommunikation.

Forts. på sid 10

Tema – INDUSTRI 4.0

Forts. från sid 8

– Datadioden kopplas så att information kan importeras till systemet, men eftersom ingen trafik tillåts i motsatt riktning kan ingen information läcka ut. Man riskerar alltså inte informationsläckage när man installerar uppdateringen.

Fotocred: Advenica

Kontorssystemen extra sårbara

En annan säkerhetsrisk som uppkommer när man jobbar mot den helt uppkopplade fabriken i industri 4.0 är att det då också finns behov av att koppla ihop produktionssystemen med de administrativa systemen för större effektivitet. Exempelvis om det prediktiva underhållet signalerar att ett kugghjul är på väg att ta slut så ska det automatiskt gå en signal till inköpssystemet att lägga upp en order på ett sådant kugghjul.

– Men detta kan ställa till det ganska rejält. Det är generellt sett svårt att nå en hög säkerhetsnivå i kontorssystemen. Penetrationstestare, ”Red Teams” och inte minst verkliga attacker visar gång på gång att dessa system är sårbara vilket gör att riskerna för attacker mot produktionen via kontorssystemen blir betydande.

Men även här kan man använda datadioder och använda olika kanaler för ingående och utgående informationsflöden.

– Att skicka ut information från produktionsprocesserna är sällan skadligt då det oftast inte finns så mycket hemlig information där. Det är den ingående trafiken som behöver kontrolleras och övervakas vilket kan göras med digitala signaturer och/eller en så kallad filtvätt bestående av två datadioder och en server för antivirusskanning. Filtvätten utgör en oberoende kontroll av att filer som importeras inte innehåller skadlig kod eller att en uppdatering är äkta.

Dela in i säkerhetszoner

En annan viktig del av säkerhetsarbetet är att tänka i zoner, områden med olika säkerhetskrav, konsekvensnivåer och kalkylerad risk att bli attackerade.

– Inne i en fabriksbyggnad kan man skydda sig relativt bra eftersom man där oftast har ett bra skalskydd, men om man har system i osäkra miljöer, som till exempel inom fjärrvärme där man har mätstationer och pumphus på osäkra platser ute i samhället som skickar information till produktionssystemet så blir dessa osäkra mätställen potentiella vägar in i systemet. De osäkra installationerna bör därför placeras i separata säkerhetszoner och de centrala styrsystemen behöver skyddas från dessa.

Som hjälp i detta finns en internationell standard IEC 62443 som på ett tydligt sätt beskriver hur man kan dela in sitt system i säkerhetszoner för att i varje zon kunna hantera potentiella risker på ett optimerat sätt relativt kostnad.

– För det får man inte glömma bort, en högre säkerhetsnivå kostar mer och därför behöver man ha koll på sina system och sin information och veta vad som är mer skyddsvärt än annat, och etablera den säkerhetsnivå som är motiverat utifrån värdet på den skyddade tillgången. Det går inte att jobba med säkerhet utan att känna sina tillgångar och göra en genomgående riskbedömning med påföljande prioritering.

Tänk efter före

Han poängterar återigen att när många nu förnyar sina system på väg mot Industri 4.0 så måste de ta med säkerhetstänket från början.

– Annars blir det som att kasta in jästen efter brödet i ugnen, att först i efterhand tänka igenom säkerhetsaspekter leder nästan ofelbart till att man behöver göra om och göra rätt. Så ett gott råd är att tänka efter före. Det är också mycket viktigt att säkerhetsfrågor hanteras i den högsta företagsledningen, de tekniska avdelningarna kan se till att jobbet blir gjort, men ansvar och prioritering måste ske på högsta nivå.

Mindre företag – ta hjälp av leverantörerna

När det gäller mindre företag med mindre resurser att lägga på säkerhetsarbete så ger han rådet att lägga över en del av bördan på leverantörerna.

– Köper man en ny smart komponent, tjänst eller system som ska installeras så är det bra om man innan köpet ställer säkerhetsrelaterade frågor som ”Hur säkerställer ni att det här systemet ni levererar inte kan hackas?”, och liknande frågor. Man ska ha förtroende för och känna tillit till leverantören och produkterna. Ansvaret kan aldrig delegeras till leverantören, det har alltid företaget självt, men jobbet och bördan med att säkerställa att det man köper in har en tillräcklig säkerhetsnivå kan absolut läggas på leverantören.

Ylva Sjönell