Sårbarheten i Log4j väcker aktuell fråga: Hur jobbar du med sårbarhetshantering?

Att upprätthålla IT-säkerheten i en industrianläggning är ett teamwork, där leverantören har sitt ansvar och kunden har sitt, i en process som pågår under anläggningens hela livscykel. ”Sårbarhetshantering är en process som måste pågå kontinuerligt så länge anläggningen är i drift om man vill undvika säkerhetshål”, säger Urban Haglund. Det blev många varse i december, då en uppdatering i Apachebiblioteket Log4j visade sig innehålla en sårbarhet.

Digitaliseringen inom industrin ger många nya möjligheter till effektivare och mer flexibel produktion med högre kvalitet och kortare ledtider. Samtidigt ökar också riskerna för cyberrelaterade angrepp som kan leda till oönskade driftstörningar, stöld av känslig information med mera.

Självklart är det viktigt att man utvärderar sin nuvarande situation och tar fram ett övergripande säkerhetskoncept med ett djupledsförsvar mot olika typer av hot att hålla sig till när man bygger eller förändrar en automationslösning.

– På Siemens har vi konsulttjänster för att hjälpa till med dessa två första steg: att analysera situationen och implementera rätt åtgärder. Men när man väl har kommit så långt och har implementerat detta kommer vi till det tredje steget, som är lika viktigt: att upprätthålla säkerheten i anläggningen under hela dess livslängd, säger Urban Haglund, Product and Solution Security Officer för Siemens i Norden.

Kontinuerlig sårbarhetsbevakning. Att upprätthålla IT-säkerheten i en anläggning handlar bland annat om att täppa till eventuella sårbarheter som kan dyka upp i produkter och system, vilket kan vara en utmaning med tanke på mängden mjukvara som dagens automationssystem innehåller. Även om en mjukvara under utvecklingsfasen har designats och testats enligt alla kända säkerhetsprinciper innan den släpps kan nya angreppsmetoder eller andra insikter innebära att en sårbarhet upptäcks efter att mjukvaran har släppts. Ett aktuellt exempel är Apachebiblioteket Log4j där en uppdatering i december visade sig innehålla en sårbarhet, något som kan drabba väldigt många då det används som komponent i många produkter.

– Man måste alltså ha en kontinuerlig sårbarhetsbevakning för komponenterna i en anläggning under hela dess livscykel. Detta gäller både hårdvara och mjukvara, säger Urban Haglund.

Behovet av effektiv sårbarhetshantering ökar. Den pågående digitaliseringen ökar behovet av att öppna upp system för extern kommunikation. Detta riskerar att öka antalet angreppsytor.

– Har man mycket mjukvara måste man räkna med risken att den kan vara eller bli sårbar. Vi ser en ökad aktivitet med angreppsförsök där också en del leder till allvarliga incidenter. Det gör att det blir viktigare att ha en aktiv process kring sårbarhetshantering, säger Urban Haglund.

IEC 62443, som är den största standarden för hantering av Cyber Security i automationssystem, föreskriver att en aktiv Patch Management-strategi behöver finnas för en automationsanläggning. Detsamma gäller informationssäkerhetsstandarden ISO 27001.

– Anläggningsägaren behöver ha en process på plats för sårbarhetshantering av sin fabriksanläggning. Att ha en anläggning utan sårbarheter är också en grundpelare för att ha en säker anläggning ur ett personsäkerhetsperspektiv, säger Urban Haglund.

Siemens arbete med sårbarhetshantering. Siemens produktutvecklingsprocess är certifierad enligt IEC 62443 4-1 för att säkerställa att utvecklingsprocessen och livscykelhanteringen av produkterna uppfyller kraven vid leverans.

– Detta inkluderar också en hantering för att upprätthålla säkerheten för produkterna och deras ingående tredjepartsmjukvara under hela livscykeln. Vår policy är att vara öppna med att publicera kända sårbarheter på våra produkter, säger Urban Haglund.

I Sverige driver Myndigheten för samhällsskydd och beredskap, MSB, ett nationellt Computer Security Incident Response Team, kallat CERT-SE, med övergripande uppgift att stödja samhället i arbetet med att hantera och förebygga IT-incidenter.

– Siemens har ett eget ProductCERT-team med säkerhetsexperter som samarbetar med olika nationella CERT-team, säkerhetsforskare med flera. Det teamet är vårt öra mot rälsen för att bevaka vad som händer inom säkerhetsområdet och hur det påverkar Siemens. De säkerställer också att våra produkter utvecklas och testas enligt de senaste rönen. På **siemens.com/cert** publiceras kända sårbarheter på Siemens produkter i så kallade Security Advisories som ger rekommendationer på åtgärder för att hantera och åtgärda sårbarheten.

Bevakar sårbarheter. Siemens har ett ansvar att leverera säkra produkter och att hålla dem säkra under hela livscykeln.

– Men det är oerhört viktigt att anläggningsägarna själva har rutiner för sårbarhetshantering. Vi vet ju inte exakt vilka som använder våra produkter eftersom många kunder handlar via systemintegratörer eller distributörer. Därför behöver alla kunder ha en sårbarhetsbevakning på sina tillgångar, såväl Siemensprodukter som produkter från andra leverantörer. En anläggningsägare behöver bevaka om nya sårbarheter upptäcks och bedöma om det påverkar anläggningen. Viktigt är att kunden själv säkerställer att den aktiviteten utförs, påpekar Urban Haglund.

Automatisk bevakning med Industrial Vulnerability Manager. Det är alltså viktigt att lyfta sig till någon form av sårbarhetsbevakning. Steg ett är att veta vad man har för hårdvara och mjukvara genom att skapa och upprätthålla en korrekt inventarielista. Därefter kan man påbörja en sårbarhetsbevakning för dessa komponenter. Att göra detta manuellt är arbetskrävande – därför har Siemens tagit fram ett verktyg, Industrial Vulnerability Manager, som ger hjälp på vägen genom att skapa en bevakningslista med automatiska bevakningar och bulletiner som upplyser när en sårbarhet upptäcks.

– Vi har en databas med både våra egna och andra leverantörers produkter och kan erbjuda en automatisk bevakning av inventarielistan. Skulle det dyka upp en sårbarhet meddelar verktyget automatiskt om sårbarheten och hjälper anläggningsägaren i processen med analys av påverkan, lämplig åtgärd och uppföljning att åtgärden genomförs. Verktyget har också en pedagogisk dashbord som beskriver övergripande status i sårbarhetsarbetet, både för Siemens produkter och andra varumärken. Att ha någon form av sårbarhetsstrategi är en nödvändig komponent i det totala säkerhetstänket, konstaterar Urban Haglund. ■

siemens.com/industrial-security
siemens.com/cert
cert.se
urban.haglund@siemens.com

Industrial Vulnerability Manager