SÄRTRYCK UR STRATEGISK UTBLICK 7

Sveriges elförsörjning

Hur möter vi en ökad sårbarhet?

Maria Andersson och Lars Westerdahl

Hela vårt samhälle har blivit starkt beroende av elförsörjning. Utan elektricitet slutar det mesta att fungera. Samtidigt är elförsörjningssystemet mycket sårbart och den pågående utvecklingen mot smarta elnät förstärker detta. Angripare kan redan ta sig in i dagens elnät i syfte att utföra cyberattacker. Dessa kan leda till stora störningar i samhället, vilket ett aktuellt exempel från Ukraina visar. Dessa ökade risker måste tas hänsyn till i den pågående omvandlingen av det svenska elförsörjningssystemet.

Elförsörjningssystemet som mål för cyberhot

Försvarets radioanstalt (FRA) meddelade i januari 2017 att man funnit spår av aktiviteter som misstänks ha varit förberedelser för cyberangrepp mot det svenska elnätet. I Ukraina skedde 2015 en cyberattack mot elnätet. Angreppet inleddes med att mejl med preparerade bilagor skickades till olika eldistributörer. Bilagorna innehöll skadlig kod vilket gjorde det möjligt för angriparna att ta sig förbi brandväggar och in i styrsystemet, och därifrån ta sig vidare till sitt huvudsakliga mål. Cyberattacken ledde till att hundratusentals abonnenter blev strömlösa. Efter några timmar kunde man manuellt återstarta elnätet.

Ett elförsörjningssystem i förändring

Det svenska elnätet håller på att utvecklas mot ett så kallat smart elnät. Smarta elnät karaktäriseras av en ökad användning av modern kommunikationsteknik. Data samlas in från fler aktörer, vilket skapar möjligheter till ingående analyser av olika tillstånd i elförsörjningssystemet. Analyserna kan bland annat ligga till grund för en mer kostnadseffektiv prissättning, förbättrade prognoser på efterfrågan samt en högre efterfrågeflexibilitet. Med smarta elnät finns goda möjligheter till förbättrad energi-effektivitet och minskade kostnader för elförsörjningssystemet. Men utvecklingen mot smarta elnät ökar även sårbarheten för cyberattacker.

Traditionella elnät distribuerar el i en riktning och produktionen är anpassad till ett schablonmässigt kundbehov. Elproduktionen har historiskt sett huvudsakligen skett i storskaliga elproduktionsanläggningar såsom vattenkraftverk och kärnkraftverk.

Smarta elnät kan ses som ett uppgraderat traditionellt elnät, där ny teknik installeras för förbättrad styrning och övervakning av alla delar av elförsörjningssystemet. Den nya tekniken gör det möjligt att bättre kunna balansera utbud och efterfrågan på el. Detta är en av anledningarna till att smarta elnät har en högre efterfrågeflexibilitet och bättre kan hantera variabel elproduktion från förnyelsebara energikällor såsom sol- och vindkraft. Ytterligare en drivkraft bakom utvecklingen mot smarta elnät är klimatpolitiken där klimatmålen i EU och Sverige ställer krav på att minska utsläppen av växthusgaser. Viktiga delar för att uppnå klimatmålen är att öka användningen av förnyelsebara energikällor och förbättra energieffektiviteten. Båda dessa områden gynnas av smarta elnät. Sammanfattningsvis så är det den storskaliga introduktionen av variabel elproduktion, samt krav på energieffektivisering och efterfrågeflexibilitet som skapat en efterfrågan på smarta elnät. I jämförelse med traditionella elät ställer smarta elnät större krav på att fler aktörer kommunicerar och samverkar med varandra.

Ökad sårbarhet

Elnätens styrsystem har traditionellt varit mer eller mindre isolerade från omvärlden. I takt med utveckling och prisfall på IT-komponenter har dessa i högre grad ersatt traditionella elektriska komponenter och företagsspecifika lösningar i styrsystem. Exempelvis används ofta hård- och mjukvarukomponenter samt kommunikationsprotokoll som från början har utvecklats för vanliga kontorssystem i de styrdatorer som används i elnätet. Denna utveckling har resulterat i att kontrollsystem och kontorssystem kan kommunicera med varandra. För affärsverksamheten i en organisation har detta inneburet en potentiellt ökad tillgång till mer aktuell information över vad som produceras. Denna information kan exempelvis användas i syfte att debitera kunden mer korrekt.

FOI Memo 6173
Godkänd av: Lena Bartholdson

Särtryck ur Strategisk utblick 7
November 2017

Sammankopplingen av system skapar inte bara ett ökat kommunikationsbehov utan ökar även exponeringen av produktions-, transmissions- och distributionssystem mot en miljö som de inte är designade att hantera. Ett ökat internt kommunikationsbehov ökar komplexiteten hos elförsörjningssystemet, samtidigt som en ökad exponering mot internet medför en öppning mot antagonistiska hot. En antagonist, det vill säga en medveten angripare som vill stjäla information, hindra tillgång till system eller utnyttja dem för egna intressen, är något som inte tidigare i någon större utsträckning behövts ta hänsyn till.

Säkerhetsfunktioner som är korrekt införda i ett system är i dagsläget svåra att ta sig förbi. Detta har medfört att angripare istället ger sig på människor genom exempelvis nätfiske (eng. *phishing*) och riktat nätfiske (eng. *spear phishing*). Dessa angrepp syftar till att lura personen som sitter vid en dator i målorganisationen att öppna en preparerad bilaga eller att klicka på en länk till en preparerad webbsida. Om angreppet lyckas, det vill säga användaren öppnar bilagan eller klickar på länken, har angriparen kommit förbi brandväggen och är inne på nätverket. Utifrån ett sådant fotfäste kan en angripare ta sig vidare mot sitt huvudsakliga mål. Elavbrottet i Ukraina 2015 är ett exempel på de sårbarheter som finns hos elförsörjningssystemet.

Behovet av strukturerat säkerhetsarbete

Risken för sårbarheter är större i komplexa system med flera aktörer. I en sådan miljö krävs ett strukturerat säkerhetsarbete mellan aktörer för att uppnå ett fullgott skydd för hela elnätet. Målet med säkerhetsarbetet är att ett system ska kunna bidra till verksamheten även om antagonister försöker angripa systemet. Detta uppnås med en kombination av utbildade människor, administrativa åtgärder och tekniska lösningar.

Ett kontinuerligt säkerhetsarbete blir särskilt angeläget för kontrollsystem med tanke på att de oftast har en lång livslängd, ibland upp till 20 år, och höga krav på tillgänglighet. Detta kan jämföras med kontorsbaserade IT-system, vilka ofta omsätts i intervallet 3–5 år. Varje aktör måste också därför arbeta systematiskt med säkerhetsfrågor för de egna systemen under hela dess livslängd.

Ett system designas för att kunna hantera kända sårbarheter. Efter hand som systemet underhålls och förvaltas kan nya sårbarheter tillkomma, till exempel genom en ökad exponering. Det innebär att ett system som inte förvaltas ur ett säkerhetsperspektiv försämras över tiden. Säkerhet är inte en produkt som tillförs ett system vid ett tillfälle, utan resultatet av ett långsiktigt och kontinuerligt arbete.

Säkerhetsanalys

Infrastruktursystem såsom elförsörjningssystem utvecklas sällan av en enskild systemägare. Flera aktörer interagerar i elförsörjningssystemet och systemet består av flera delsystem som behöver ta hänsyn till varandra. Förändringar i dessa delsystem sker inte samtidigt, vilket medför att nya och gamla delsystem behöver kunna utbyta information med varandra, och kan även ha beroenden mellan sig.

Att bygga IT-system för en miljö där det finns flera system med olika ägare ställer stora krav på gränsytorna mellan systemen för att kommunikation ska vara möjlig. Varje aktör måste säkerhetsställa sitt delsystems funktion samt identifiera vilka risker delsystemet utsätts för. Det är därför viktigt att delsystemägare har en gemensam syn på den hotbild deras system ska verka under. När ett nytt system ska införas blir säkerhetsanalysen ett viktigt verktyg för att identifiera vilka säkerhetsfunktioner som behövs och vilka rutiner som behöver stödja dessa.

Säkerhetsarbetet upphör dock inte när systemet tas i bruk, eftersom säkerheten i ett system kommer att försämras med tiden. IT-system innehåller svagheter som upptäcks efter hand och korrigeras genom uppdateringar (så kallad *patchning*). Om dessa uppdateringar inte installeras kommer systemet att innehålla kända svagheter.

Ett system som förvaltas förändras kontinuerligt vilket medför att nya säkerhethetsanalyser behöver genomföras kontinuerligt. Den funktionalitet som tillförs ett system efter att det tagits i bruk behöver granskas lika noggrant som nya funktioner görs under systemets utveckling.

Att förebygga cyberattacker

De grundläggande förutsättningarna för säkerheten i ett system skapas under systemets utveckling och genom underhållsarbete. Därutöver behövs ett aktivt säkerhetsarbete under systemets användning, med förebyggande och uppföljande aktiviteter över tiden.

FOI
Totalförsvarets forskningsinstitut
SE-164 90 Stockholm

Phone: +46 8 5550 3000
Fax: +46 8 5550 3100
www.foi.se/om-foi/strategisk-utblick

Ökad säkerhet uppnås med hjälp av tekniska lösningar, administrativa rutiner och en stödjande organisation.

Administrativa rutiner ger struktur åt säkerhetsarbetet. Det strukturerade säkerhetsarbetet fokuserar dock inte enbart på den funktionalitet som systemet ska leverera, utan även den funktionalitet som systemet faktiskt har. Det innebär att systemägaren måste känna till vad som finns installerat i systemet och vårda all funktionalitet alternativt ta bort sådant som är onödigt. Kontroll av underhållsarbetet, exempelvis installerade uppdateringar, är en del av säkerhetsarbetet.

I samverkande system, till exempel i elnäten där det finns flera aktörer, blir det ännu viktigare att aktivt övervaka de egna nätverken. De säkerhetsfunktioner som har tillförts i utvecklingsfasen är designade att hantera den hotbild om fanns när systemet togs fram. För ett system som varit i drift ett tag kan nya hot ha uppstått, vilka de gamla säkerhetslösningarna inte alltid kan upptäcka eller hantera. Det blir därför viktigt att exempelvis vara uppmärksam på förändringar i kommunikationsmönster i de egna nätverken. För att upptäcka otillåten aktivitet på nätverket behövs övervakning, som exempelvis loggning, intrångsdetekteringssystem och anti-virusprogram, men också personal som kan följa upp loggar och larm.

Att hantera cyberattacker

Ett upptäckt angrepp behöver hanteras, oavsett om det syftar till informationsstöld, att förhindra åtkomst eller att utnyttja systemfunktioner för egna syften. Hur denna hantering ska gå till beror på vilken typ av funktionalitet som systemet levererar. I ett informationssystem utan hårda tidskrav kan man välja att ta systemet ur drift för att åtgärda intrånget. Men för ett system som stödjer kritisk infrastruktur, såsom elnät, är detta inte alltid möjligt. I sådana fall får angreppet hanteras samtidigt som systemet fortsätter att stödja organisationens verksamhet.

Nyckeln till att hantera ett angrepp effektivt är förberedelser. En etablerad krisgrupp baserad på ett antal nyckelpersoner med god kännedom om verksamheten och med ett stort kontaktnät är en viktig resurs i ett sådant läge. Gruppen måste vara förberedd genom att i förväg ha gått igenom ett antal möjliga fall och ha upprättat handlingsplaner, kontaktlistor, med mera. En sådan grupp behöver inte enbart finnas till för att hantera cyberattacker utan kan vara en tillgång som ”allmän brandkår” inom en organisation.

Större organisationer kan etablera en fast grupp med hög teknisk kompetens för att hantera IT-problem, ett så kallat *Computer Emergency Response Team* (CERT). Dess uppgift är i första hand att så snabbt och effektivt som möjligt återställa ett angripet system och i andra hand att se till att samma problem inte uppstår igen. En CERT är kostsam att ha så dessa tenderar att vara branschsamarbeten eller nationella funktioner. Som externa resurser kan de stödja mindre organisationer med teknisk kompetens och kunskap om kända hot.

Smarta elnät innebär en högre exponering av styrfunktionalitet vilket ger en större angreppsyta mot systemen. Angreppsytan behöver dock inte medföra att det ställs krav på andra säkerhetsfunktioner i systemet. Däremot kan högre krav ställas på förmågan att upptäcka intrång i de egna systemen jämfört med tidigare, samt att kunna hantera incidenter. Ett ökat antal aktörer inom elförsörjningssystemen ställer dessutom högre krav på samordning av säkerhetsfrågor.

Det nya elförsörjningssystemet kräver både nya och gamla säkerhetslösningar

Det finns flera starka drivkrafter bakom utvecklingen mot smarta elnät, och utvecklingen kan komma att gå snabbt. Det är viktigt att inleda ett både intensifierat och strukturerat säkerhetsarbete redan i utvecklingsfasen, och att arbetet fortgår under elnätens hela livslängd. Ett aktivt säkerhetsarbete – där människor, administrativa rutiner och teknik samverkar – är en nödvändighet för IT-system med långa livslängder. Det medför att ett aktivt säkerhetsarbete är viktigt så länge systemet är operativt.

Angreppet mot elnätet i Ukraina 2015 exemplifierar väl detta behov. Även om bortfallet av el bara var några timmar hade angreppet pågått i flera månader. Det är vanligt att cyberattacker förblir oupptäckta i flera månader, ibland år, beroende på angriparens mål. I Ukrainafallet inleddes angreppet med en riktad nätfiskeattack i syfte att få ett fotfäste i nätverken. Därefter vidtog en lång period av spaning i nätverken i syfte att hitta en väg från den inledningsvis övertagna datorn till det faktiska målsystemet. Det är under denna period som ett aktivt säkerhetsarbete med övervakning skulle kunna ha upptäckt angreppet.

FOI
Totalförsvarets forskningsinstitut
SE-164 90 Stockholm

Phone: +46 8 5550 3000
Fax: +46 8 5550 3100
www.foi.se/om-foi/strategisk-utblick

Det svenska elnätet, likt mycket annan kritisk infrastruktur, består av flera aktörer. Det är därför viktigt att incidenter kan rapporteras till en organisation där en överblick kan uppnås.

Händelserna i Ukraina påvisar också en annan viktig lärdom – att det är fortfarande viktigt med manuella återställningsfunktioner. För att få igång eldistributionen igen var teknikerna tvungna att tillfälligtvis återgå till manuella funktioner.

För vidare läsning

Admund Gudmunsson Hunstad, och Martin Karresand, *Monitorerings- och övervakningssystem*, 2017, FOI-R--4420--SE.

Jessica Johansson, *Litteraturstudie – Risk- och sårbarhets-analyser i smarta elnät*, 2013, FOI Memo 4500.

***Strategisk utblick 7* finns att ladda ner från www.foi.se/om-foi/strategisk-utblick**

FOI
Totalförsvarets forskningsinstitut
SE-164 90 Stockholm

Phone: +46 8 5550 3000
Fax: +46 8 5550 3100
www.foi.se/om-foi/strategisk-utblick