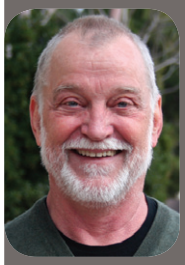
Målrettede angrep – er kraftbransjen forberedt?

Av MARIA B. LINE
Stipendiat ved NTNU og forsker ved SINTEF IKT.

Av ALI ZAND
Stipendiat ved University of California Santa Barbara.

Av GIANLUCA STRINGHINI
Førsteamanuensis ved University College London.



Av RICHARD A. KEMMERER
Professor ved University of California Santa Barbara.

Nettselskapene er ikke godt nok forberedt på målrettede angrep, ikke en gang godt nok forberedt på å møte tradisjonelle IT-sikkerhetstrusler. Det viser en studie foretatt av artikkelforfatterne.

Foto: Sigurd Aarvig

Fysiske angrep er kraftbransjen godt forberedt på, men IT-angrep, og spesielt avanserte målrettede angrep, har ikke vært høyt nok oppe på agendaen.

Målrettede angrep er en økende trend, og kraftindustrien er et attraktivt mål. Spionasje eller fysiske ødeleggelser kan typisk være hensikten med slike angrep. Konsekvensene kan bli fatale: store områder, inkludert kritisk samfunnsinfrastruktur, kan rammes av strømbrudd.

Vi har studert og kategorisert velkjente målrettede angrep. Deretter har vi utført en intervjustudie blant norske nettselskap for å vurdere hvor godt forberedte de er på å oppdage og respondere på slike angrep. Våre funn tyder på at kraftbransjen er godt forberedt på tradisjonelle, fysiske angrep, men IT-angrep, og spesielt avanserte målrettede angrep, har ikke vært høyt nok oppe på agendaen deres foreløpig. Ved å forstå kjente angrep og lære fra dem, håper vi på å hjelpe bransjen med å forbedre deres evner til å oppdage og respondere på målrettede angrep.

Målrettede angrep

Målrettede angrep er gjerne vanskelig å oppdage. De utføres over lang tid, hvilket gjør dem vanskelig å identifisere av vanlige deteksjonssystemer. Dessuten bruker angripere gjerne ulike teknikker for sosial manipulering for å kartlegge organisasjonen som skal angripes, samt dens IT-systemer. Slike teknikker lar seg ikke oppdage av deteksjonssystemer. Videre er ikke nødvendigvis de aller nyeste verktøyene i bruk blant organisasjoner.

Målrettede angrep inkluderes gjerne i risikovurderinger, og selv om de har svært alvorlige konsekvenser, har de også en relativt lav sannsynlighet. Derfor er det vanskelig for en organisasjon å vurdere i hvor stor grad de skal prioritere sikkerhetsmekanismer som kan hindre slike angrep. Det kan være andre typer angrep/hendelser som har høyere sannsynlighet og som dermed prioriteres høyere på tiltakslista.

Vi har sett nærmere på fire kjente målrettede angrep: NightDragon, Operation Aurora, Careto og Stuxnet. Ut ifra disse har vi identifisert fire egenskaper ved slike målrettede angrep:

- hensikt med angrepet: sabotasje eller uthenting av konfidensiell informasjon
- første steg: automatisk (for eksempel drive-by download av malware) eller manuell (krever en handling fra en på innsiden)
- neste steg, etter å ha oppnådd tilgang på innsiden: automatisk eller manuell
- plassering av Command& Control-server: på innsiden av eller utenfor organisasjonens nettverk

Cyber situation awareness

CSA handler om forståelse på ulike nivå: 1) hensikten med egne IT-systemer, hvordan de fungerer og hvilke avhengigheter som finnes mellom ulike komponenter, 2) hendelser i nettverket og 3) trusler, hvordan de truer hensikten med systemene, og hvordan de kan forebygges eller reageres på.

Ulike verktøy og metoder kan brukes for å oppnå en slik forståelse, blant annet innbruddsdeteksjon, et system som korrelerer alarmer og ser sammenhenger, analyse av angrepstrender, sårbarhetsanalyser, årsaksanslyser.

Vi har intervjuet sikkerhetsansvarlige for kontrollsystemer i seks større norske nettselskap. Spørsmålene utviklet vi basert på teori fra CSA, og intervjuobjektene fikk tilsendt spørsmålene på forhånd.

Funn

Alle nettselskapene hadde god innsikt i hensikten med egne systemer og avhengigheter mellom ulike komponenter. Omfanget av systemene er relativt begrenset, og de er pålagt å utføre både risikovurderinger og avhengighetsanalyser. De har dessuten en god forståelse av behovet for å sikre kontrollsystemene mot generelle informasjonssikkerhetstrusler. Nettselskapene har imidlertid ikke gode verktøy for å oppdage og overvåke hendelser på innsiden av kontrollsystemene sine. Deteksjonssystemer er i bruk i begrenset omfang, og ingen har systemer for å korrelere alarmer og se sammenhenger. De har brannmurer som kan være i stand til å oppdage mistenkelig trafikk til og fra nettverket, men dersom angriper greier å komme seg forbi denne, kan han operere på innsiden uten å bli overvåket. Det er bred felles enighet om at kontrollrommet kan kobles av nett dersom de opplever angrep. Dette krever imidlertid at angrepet oppdages.

Sannsynligheten for å bli rammet av målrettede angrep anses som svært lav, delvis fordi det foreløpig ikke har vært opplevd blant noen i bransjen. Sannsynligheten for fysiske angrep vurderes som høyere.

Kun ett av de seks nettselskapene har gjennomført beredskapsøvelse med utgangspunkt i en IT-sikkerhetshendelse.

Tre av nettselskapene bruker såkalte IPS – intrusion prevention systems. Disse er imidlertid kjent for å generere et høyt antall alarmer. Det innrømmes at det ikke finnes ressurser til jevnlig oppfølging av slike alarmer. En svakhet ved brannmurer og IPS er dessuten at de er best på å oppdage angrep som er kjent fra før. Nye angrep, for eksempel angrep som er spesialdesignet og målrettet, vil ikke kunne oppdages med slike verktøy.

Anbefalinger

Vi har utarbeidet en prioritert liste med anbefalinger til nettselskapene ut fra hvordan vi vurderer deres evner og muligheter til å oppdage og respondere på målrettede angrep i dag:

1. Gjennomfør beredskapsøvelser basert på IT-sikkerhetshendelser jevnlig. Det er et paradoks at alle nettselskapene er enige om hva som vil være den verst mulige hendelsen, men ingen likevel har øvd på dette scenariet.

2. Vær i stand til å oppdage og stå imot angrep basert på sosial manipulering. Dette krever bevisste ansatte på alle nivå i organisasjonen. Det finnes ingen 1–2–3-løsning på hvordan man skal få til dette, det krever kontinuerlig innsats og bevisstgjøring. Samtidig er sosial manipulering svært effektivt for angripere som ønsker informasjon.

3. Ha et fysisk skille mellom kontrollsystemene og andre IT-systemer i den grad det er mulig. Vi er fullstendig klar over at utviklingen går den andre veien av hensyn til effektivitet og funksjonalitet. Vi vil likevel påpeke at det ikke er anbefalt fra et sikkerhetsståsted.

4. Ta i bruk systemer for avviksdeteksjon. Dette er svært effektivt for eksempel for kontrollsystemer som i stor grad inneholder forutsigbare hendelser.

5. Bruk myndighetspålagte tiltak for å sikre forbedringer. Tiltak som er pålagt fra myndighetene, blir i stor grad etterlevd. Myndighetene har derfor et stort ansvar i å stille riktige og tilstrekkelige krav.

Vår studie viser at nettselskapene ikke er godt nok forberedt for målrettede angrep i dag. De er ikke en gang godt nok forberedt på å møte tradisjonelle IT-sikkerhetstrusler. De mangler verktøy for å overvåke og oppdage angrep, samt systematisk oppfølging av logger og varsler.

Studien ble utført av Maria B. Line, Ali Zand, Gianluca Stringhini og Richard A. Kemmerer i mars–mai 2014 i samarbeid mellom NTNU og UCSB, med delfinansiering fra Norges forskningsråd.