SVENSKA KRAFTNÄT

Informationsklass
K1

Kristina Westerdahl

2021-02-08 2020/396

It-attacker mot aktörer i elsektorn: lägesbild och trend

Innehåll

1 Bakgrund

Attacker, via internet eller på annat sätt, och mot it-system (it-attacker) är aktuella risker för alla som använder internet och it-system. Angreppen varierar dock över tid. Under det senaste året har angrepp med utpressningsprogram (även kallat ransomware) ökat och ändrat karaktär.

Två av de mest kända it-angreppen mot elsektorn är de som drabbade Ukraina 2015 och 2016. De orsakade elavbrott för ett stort antal konsumenter under vintern när även kortare avbrott kan vara kännbara.[1]

För att bidra till bedömningar av risken för it-angrepp följer här en sammanfattning av angrepp som drabbat elsektorn efter 2016, främst med fokus på Europa. Sammanfattningen baseras på öppna källor. Eftersom angreppen inte alltid offentliggörs är den inte heltäckande och särskilt för nyligen inträffade händelser är informationen ofta begränsad.

2 Sammanfattning av angrepp i elsektorn

2.1 Elaktörer som har angripits

Under 2017-2020 har en rad olika aktörer i elsektorn drabbats av it-angrepp. Åtminstone en kraftproducent har angripits. Flera operatörer av transmissionsnät och regionnät har drabbats. Även elmarknadsföretag och leverantörer av kontrollutrustning bl.a. för SCADA-system, samt av ledningar och kablar.

2.2 Angriparnas tillvägagångssätt

Minst sex fall av introduktion av skadlig kod hos elaktörer rapporterades i öppna medier 2017-2020. Ibland är angriparens syfte med skadlig kod oklar. I de fall som rör elaktörer där syftet kan identifieras, handlar det om utpressning (s.k. Ransomware) och datastöld inklusive industrispionage.

I fall med skadlig kod har sannolikt någon med behörighet till aktörens it-system medverkat till införande av den skadliga koden, t.ex. genom phishing. Det finns även ett exempel på utnyttjande av s.k. bakdörrskonton som är till för att säkra administratörsrättigheter och kontroll i katastroflägen. Andra sårbarheter som möjliggjort angrepp tros vara icke installerade säkerhetsuppdateringar.

Angrepp med skadlig kod förefaller vara det vanligaste tillvägagångssättet men exempel på intrång i IKT-system förekommer också.

[1] MSB, ”Viktiga lärdomar från elavbrotten i Ukraina”, 201703 (https://www.msb.se/contentassets/6840a9f762184a869b39954f670c8e77/lardomar-fran-ukrainska-elavbrott.pdf)

2.3 Angripare

Angriparna tillhör två huvudsakliga kategorier: kriminella respektive statligt stödda grupper. Kriminella drivs framförallt av ekonomiska intressen och använder sig av t.ex. ransomware. Statsstödda gruppers intresse förefaller vara tillgång till it-system, dvs. en förmåga att styra it-system och industriella processer, samt inhämtning av information.

2.4 Konsekvenser

De identifierade angreppens konsekvenser varierar från inga märkbara effekter till kryptering av filer och system samt risker för omfattande skador på egendom och människoliv. I fall med ransomware har angriparna publicerat information de kommit över hos den drabbade organisationen, t.ex. lösenord samt medarbetares inloggningsuppgifter och konton. I ett fall beskrivs informationen som ”mycket känslig” och ”konfidentiella filer och uppgifter”. Omfattningen på den information angriparna påstås ha kommit över hos elaktörer varierar från 120 GB till 10 TB. I de fall begärda lösensummor anges i öppna källor är de i storleksordningen 5-10 miljoner USD.

3 Trend: Ransomware

3.1 Utveckling av angrepp

Typiskt för ransomware (utpressningsprogram) är att det krypterar filer hos den drabbade organisationen och att angriparen kräver en lösensumma för att tillhandahålla information som gör att filerna ska kunna dekrypteras. Det har även förekommit att rent sabotage har maskerats att framstå som ett ransomware-angrepp, dock utan att erbjuda någon reell möjlighet att kunna dekryptera filerna (NotPetya, 2017).

EU:s myndighet för cybersäkerhet, ENISA, bedömer i sin senaste översikt av cyberhot att det inte är en fråga *om* man drabbas utan *när* man drabbas av ransomware, mot bakgrund av det ökande antalet angrepp under 2019[2].Under 2020 finns det flera angrepp med ransomware där angriparna hämtat ut filer från den drabbade organisationen före krypteringen. Angriparen har sedan spridit sådana filer för att ytterligare sätta press på den drabbade organisationen att betala lösensumman. Exempel på detta under 2020 är att patientinformation från ett vårdföretag i Finland offentliggjordes[3] och liknande angrepp förekommer även i elsektorn. Även företag i IT-branschen drabbas, bland annat det stora tyska

[2] ENISA, ”ENISA Threat Landscape 2020 - Ransomware”, 20201020 (https://www.enisa.europa.eu/publications/ransomware/at_download/fullReport)

[3] Svenska Dagbladet, ”Patienter utpressas efter hackning i Finland”, 20201025 (https://www.svd.se/patienter-utpressas-efter-hackning-i-finland)

mjukvaruföretaget Software AG som angreps i oktober 2020[4]. I USA i december 2020 angreps it-säkerhetsföretaget FireEye[5] och mjukvaruföretaget SolarWinds[6].

När angripare har tillägnat sig (exfiltrerat) offrets filer inför kryptering med ransomware kan de begära lösensumma både för avkryptering hos organisationen och radering av de exfiltrerade filerna. Det har hänt att drabbade organisationer som betalat lösensumman inte fått det som utlovats, enligt ENISA i hälften av fallen[7].

Enligt ENISA är det en trend under 2018 och 2019 att ransomware-angrepp riktas mot statliga organisationer[8]. En annan trend är att större och därmed kapitalstarka organisationer angrips och lösensummornas belopp har ökat vilket lyfts av bl.a. Säkerhetspolisen[9]. Under 2019 betalades minst 10 miljarder EUR i lösensummor[10] och ransomware kommer sannolikt fortsätta att vara ett hot. Ett säkerhetsföretag uppskattar att angreppen kommer att leda till kostnader på mellan 20 och 22 miljarder kronor för svenska företag under 2020[11].

Angrepp med ransomware är kostsamma även om någon lösensumma inte betalas. Angreppet mot aluminiumtillverkaren Norsk Hydro i mars 2019 slog ut datorer och produktion, vilket ledde till kostnader uppemot 500 miljoner kronor enligt företaget. Det danska rederiet Maersk drabbades 2017 av ransomware som slog ut företagets it-system över hela världen och ledde till kostnader på mellan två och tre miljarder kronor.[12]

Det finns dessutom en förhållandevis stor risk att drabbas hårt av denna typ av angrepp, även om de inte är specifikt riktade mot den egna organisationen, om man inte har byggt upp en säkerhetsmässigt robust intern it-miljö och en säkerhetsmedveten användarbas. Om adekvata interna barriärer saknas mellan olika it-miljöer kan det vara möjligt för ett angrepp att sprida sig till för

[4] CPO Magazine, ”Clop Ransomware Attack Hits German Software Giant Software AG; Confidential Documents Stolen, $23 Million Ransom Demanded”, 20201019 (https://www.cpomagazine.com/cyber-security/clop-ransomware-attack-hits-german-software-giant-software-ag-confidential-documents-stolen-23-million-ransom-demanded/)

[5] The Guardian, “US cybersecurity firm FireEye says it was hacked by foreign government”, 20201209 (https://www.theguardian.com/technology/2020/dec/08/fireeye-hack-cybersecurity-theft)

[6] Tech World, ”SolarWinds hackat en vecka efter FireEye – skadlig kod i företagets uppdateringar”, 20201214 (https://techworld.idg.se/2.2524/1.744613/solarwinds-hackat)

[7] Svenska Dagbladet, ”Cyberangrepp för 20 miljarder i Sverige”, 20200629 (https://www.svd.se/svenska-notan-for-cyberangrepp-20-miljarder); ENISA, ”ENISA Threat Landscape 2020 - Ransomware”, 20201020 (https://www.enisa.europa.eu/publications/ransomware/at_download/fullReport)

[8] ENISA, ”ENISA Threat Landscape 2020 - Ransomware”, 20201020 (https://www.enisa.europa.eu/publications/ransomware/at_download/fullReport)

[9] Säkerhetspolisen, ”Cybersäkerhet i Sverige – Hot, metoder, brister och beroenden”, 20200603 (https://www.sakerhetspolisen.se/download/18.f2735ce171767402ba202/1591164566288/Rapport-Cybersakerhet-Hot-Metoder-Brister.pdf); Svenska Dagbladet, ”Cyberangrepp för 20 miljarder i Sverige”, 20200629 (https://www.svd.se/svenska-notan-for-cyberangrepp-20-miljarder); SC Magazine, ”Ragnar Locker’s well-conceived ransomware attack on Energias de Portugal”, 20200416 (https://www.scmagazine.com/home/security-news/ransomware/ragnar-lockers-well-conceived-ransomware-attack-on-energias-de-portugal/); CPO Magazine, ”Clop Ransomware Attack Hits German Software Giant Software AG; Confidential Documents Stolen, $23 Million Ransom Demanded”, 20201019 (https://www.cpomagazine.com/cyber-security/clop-ransomware-attack-hits-german-software-giant-software-ag-confidential-documents-stolen-23-million-ransom-demanded/)

[10] ENISA, ”ENISA Threat Landscape 2020 - Ransomware”, 20201020 (https://www.enisa.europa.eu/publications/ransomware/at_download/fullReport)

[11] Svenska Dagbladet, ”Cyberangrepp för 20 miljarder i Sverige”, 20200629 (https://www.svd.se/svenska-notan-for-cyberangrepp-20-miljarder)

[12] Svenska Dagbladet, ”Cyberangrepp för 20 miljarder i Sverige”, 20200629 (https://www.svd.se/svenska-notan-for-cyberangrepp-20-miljarder)

verksamhetens nyttoproduktion kritiska system, något som givetvis kan vara förödande för en aktör inom elsektorn.

3.2 Utveckling i Sverige

Ett ransomware kallat WannaCry användes 2017 för ett stort antal angrepp över hela världen under en kort tid. Även organisationer i Sverige drabbades, men endast Timrå kommun och företaget Sandviken är hittills nämnda i media.[13]

Säkerhetsföretaget Gunnebo drabbades av ett it-intrång i augusti 2020. Uppgifter tyder på att det var ett organiserat angrepp med ett ransomware kallat Mount Locker[14]. Angriparen kom över en stor mängd information som de kräver en lösensumma för att inte offentliggöra. När företaget vägrade betala har 19 gigabyte information motsvarande över 38 000 filer publicerats på internet. Den stulna informationen omfattar t.ex. finansiell information, kunddata, uppgifter om anställda, källkod till mjukvara, lösenord och ritningar över lokaler med säkerhetslösningar. En del av informationen som stals och offentliggjordes uppges vara belagd med sekretess.[15]

I november 2020 drabbades flera stora svenska företag av ransomware. Upp till 200 datorer i minst ett dussin företag berördes. Angreppen skedde under ca en veckas tid.[16]

4 Avslutande kommentarer

It-attacker är en påtaglig risk för alla organisationer och aktörer och elsektorn är inget undantag som sammanställningen visar. Det är talande att ENISA, EU:s cybersäkerhetsmyndighet, menar att det inte är en fråga *om* man kommer att drabbas utan *när*[17]. Den typ av angrepp som beskrivs här offentliggörs inte alltid och publik information innehåller ofta relativt lite uppgifter om angreppet. Sammanställningen här ger en bättre bild av risker än beskrivningar av enskilda fall och den kan användas som underlag för diskussioner om relevanta skyddsåtgärder.

[13] SVT, ”Datasäkerhetsblogg: 40 platser i Sverige drabbade av cyberattacken”, 20170513 (https://www.svt.se/nyheter/inrikes/datasakerhetsblogg-40-platser-i-sverige-drabbade-av-cyberattacken)

[14] HackRead, ”Mount Locker ransomware group leaks 18Gb worth Gunnebo AB data”, 20201029 (https://www.hackread.com/mount-locker-ransomware-group-gunnebo-ab-data/)

[15] Dagens Nyheter, ”Enorm säkerhetsläcka – hemliga uppgifter om riksdagen och banker ute på nätet”, 20201027 (https://www.dn.se/ekonomi/enorm-sakerhetslacka-hemliga-uppgifter-om-riksdagen-och-banker-ute-pa-natet/)

[16] Sveriges radio, ”Omfattande it-attack mot flera stora svenska företag”, 20201112 (https://sverigesradio.se/sida/artikel.aspx?programid=83&artikel=7598006)

[17] ENISA, ”ENISA Threat Landscape 2020 - Ransomware”, 20201020 (https://www.enisa.europa.eu/publications/ransomware/at_download/fullReport)