FAKTA

Nr 11 09/2019

Metode for å finne kraftsensitiv informasjon på Internett

Digitalisering medfører at mange publiserer informasjon om virksomhetene. Ved hjelp av metoder og digitale verktøy kan virksomhetene selv identifisere kraftsensitiv informasjon på internett. Fjerning av sensitiv informasjon eksponert på internett reduserer risikoen for cyberangrep.

ETTERRETNINGSTRUSSELEN - EN SIKKERHETSUTFORDRING

Fokus-rapporten utgitt av Forsvarets etterretningstjeneste i 2019 sier at etterretningstrusselen er den mest pågående og omfattende sikkerhetsutfordringen mot Norge og norske interesser. Man eksponerer seg selv mer, samtidig øker andelen systemkomponenter som blir koblet opp til internett. Også NSM trekker i sin rapport Risiko 2019 frem at sivil sektor er utsatt for økt eksponering av risiko gjennom økt digitalisering. NSM er opptatt av at mange virksomheter ikke har oversikt over egne sårbarheter og egen risiko. I rapporten[1] går NSM gjennom ulike risikoreduserende tiltak. En sektor som rommer kritisk infrastruktur og høyteknologi er kraftsektoren. Sensitiv informasjon som kan brukes til å skade anlegg, system eller påvirke funksjoner som har betydning for kraftforsyningen, er underlagt taushetsplikt[2] og skal beskyttes.

ER SIKKERHETEN GOD NOK?

Norsk senter for informasjonssikring (NorSIS) sin rapport[3] om nordmenn og digital sikkerhetskultur viser at 71% ikke har fått opplæring i informasjonssikkerhet i løpet av de siste 2 årene, og kun 44% bruker forskjellig passord for de fleste tjenester på nett. Samtidig viser NVEs rapport[4] fra 2017 at den vanligst oppgitte grunnen til uønskede sikkerhetshendelser i kraftbransjen er menneskelige feil eller kunnskapsmangel. Setter man disse tallene i sammenheng, kan man spørre om sikkerhetskulturen i bransjen er god nok? Ansatte eksponerer seg selv i større grad gjennom diverse sosiale medier, og å jobbe fra kafe, hjemme eller fra andre usikre nettverk, blir vanligere. Amerikanske TechRepublic skriver i en artikkel[5] at 1 av 7 organisasjoner har erfart at en kompromittert bruker i organisasjonen har sendt en «phishing» e-post til andre

[1] NSM Risiko 2019 *Krafttak for et sikrere Norge*
[2] Energiloven § 9-3
[3] Malmedal, B. (2018) *Nordmenn og digital sikkerhetskultur*, NorSIS
[4] NVE (2017) *Informasjonssikkerhetstilstanden i energiforsyningen*, NVE-rapport 90:2017
[5] Sanders, J. (2019) *Lateral phising: Hackers are taking over business accounts to send malicious emails,* TechRepublic

NVE har ansvar for å forvalte landets vann- og energiressurser, utvikle samfunnets evne til å håndtere flom- og skredfare og varsle om naturfare. NVE har hovedkontor i Oslo og regionkontor i Narvik, Trondheim, Hamar, Førde og Tønsberg. I tillegg har vi senter for fjellskredovervåking i Stranda og Kåfjord. Faktaarket er utarbeidet av Vemund Losnedal, Jarl Christophe Skrivarhaug – Boudier og Kasper Kallseter, juli-august 2019.

NVE hovedkontor
Middelthunsgt. 29
Postboks 5091, Majorstuen
0301 Oslo
Telefon: (+47) 22 95 95 95
nve@nve.no

innad i organisasjonen. Sett i sammenheng med Aftenposten sin avsløring[6] om at 1,4 milliarder passord, hvorav minst 573 000 norske, er lekket i en søkbar database på internett, må ansatte i norske virksomheter i større grad tenke sikkerhet i fremtiden.

VI KAN BRUKE ANGRIPERNES METODER

Andre nasjonsstater regnes som den største trusselaktøren, men angrepsspekteret er bredt. Kriminelle, organiserte grupper og enslige hackere drevet av å spre politiske budskap, hevn eller kredibilitet i miljøet kan skape forstyrrelser. Selve angrepet kan ha flere former. Med nok informasjon om en ansatt med tilgang til kritiske systemer kan en trusselaktør sende en målrettet e-post med oppfordring eller fristelse til å trykke på en link og laste ned skjult skadevare. Trådløst tastatur og datamus som bruker radiomottaker, kan kompromitteres og fjernstyres fra bygningens utside. Åpne printere koblet til internett kan aksesseres og overvåkes. Variasjonen av angrep er stor, og det samme blir definisjonen av informasjon som skal beskyttes.

Felles for alle angrep er imidlertid at en angriper må gjennom en rekognoseringsfase før et angrep kan finne sted. I denne fasen kan trusselaktøren bruke forskjellige etterretningsverktøy til å skaffe nyttig informasjon om virksomheten og dens systemer. Letingen dekker ansatte, leverandører, underleverandører og andre slik som media, myndigheter, akademia m.fl. Trusselaktører kan kontinuerlig overvåke nettsider som arkiverer kjente sårbarheter med systemer, og vente på at «riktig» sårbarhet dukker opp. Dette er de tre første stegene i modellen ICS-Cert presenterer i sitt kurs i angrepsmetodologi[7]; «Research», «Discovery» og «Vulnerability exploit». Modellen er vist i figur 1. De tre neste stegene som fullfører syklusen er «Maintain access», «Access escalation» og «Covering tracks». De tre første stegene baseres ofte på målbevisst bruk av verktøy som er åpent tilgjengelig på internett – en metode som kalles «Open source intelligence» (OSINT). Denne metoden kan også virksomhetene bruke i sitt eget forebyggende sikkerhetsarbeid[8].

Figur 1: Etterretning før cyberangrep er en kontinuerlig prosess. Angrepsmetoden er hentet fra ICS-Cert, USA.

METODE FOR REVISJON FOR KRAFTSENSITIV INFORMASJON

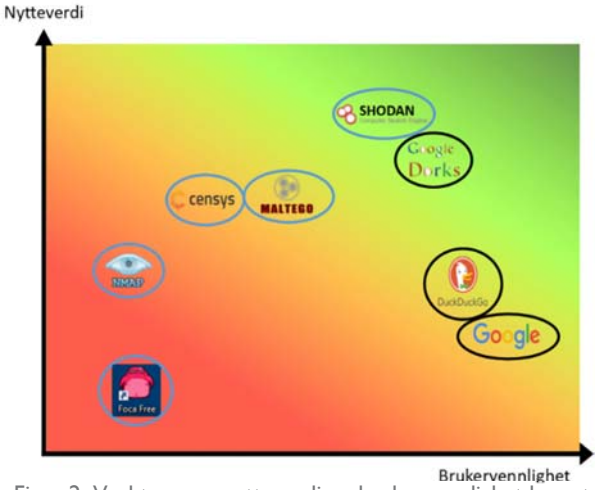
Tre sommerstudenter ved NVE med forskjellig studiebakgrunn brukte OSINT-metoder til å kartlegge hva som finnes av kraftsensitiv informasjon på internett. Oppgaven ble løst som case-studier, hvor 3 selskaper i kraftsektoren av forskjellig størrelse ble kartlagt. Studentene ble utfordret til å skissere en metode som i fremtiden kan komplementere NVEs tilsynsmetodikk, og inngå i virksomheters egne sikkerhetsrevisjoner.

DIGITAL VERKTØYKASSE

Studentene valgte å klassifisere søkemotorene i to kategorier; enkle- og avanserte søkeverktøy. De enkle verktøyene består av søkeverktøy som de aller fleste mestrer. **Google Dorks** er en slik søkemotor. Google Dorks er en utvidet funksjonalitet fra Google som lar en filtrere søk på blant annet filetype, domene og publiseringsdato. Et eksempel er å søke «filetype:xls intext:brukernavn», som resulterer i Excel-filer med brukernavn. En annen nyttig søkemotor er **DuckDuckGo**[9], som i motsetning til Google ikke lagrer informasjon om brukeren som tilpasser søk personlig. Også **offentlig informasjon** tilgjengelig via kart, databaser, rapporter, konsesjonssaker m.m. er en rikholdig informasjonskilde. Offentlige registre som **NVE Atlas**[10] inneholder kartlegging av Norges sentral- og regionalnett, og **Google Street view**[11] gir en mulighet til å «fjernvurdere» fysiske sikkerhetstiltak og bygningstilstand. **Konsesjonssøknader**[12] kan inneholde sensitiv informasjon om eksisterende anlegg som nøyaktig kartfesting av kabler eller lokalisering og plantegninger av driftsanlegg. Disse blir lagt ut til offentlig gjennomsyn både hos NVE, kommune og

[6] Furuly, J. G. (2019) *1.4 Milliarder passord lekket i søkbar database – en rekke profilerte nordmenn rammet.* Aftenposten
[7] ICS-CERT, 210W-09: «Attack Methodologies in IT & ICS»
[8] Losnedal, V. & Kallseter, K. & Boudier, J.C. (2019) *Revisjon av kraftsensitiv informasjon på internett*, NVE. (U.OFF.)
[9] *https://duckduckgo.com/*
[10] *https://atlas.nve.no/*
[11] *https://mapstreetview.com/*
[12] *https://www.nve.no/konsesjonssaker/*

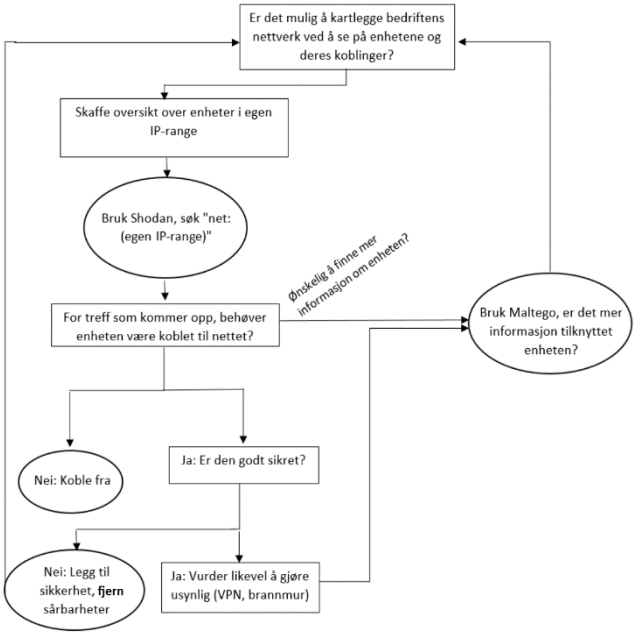
søker. **Doffin**[13] er den nasjonale kunngjøringsdatabasen for offentlige anskaffelser, og inneholder anbud som kan avsløre komponent- og systemanskaffelser.



Figur 2: Verktøyenes nytteverdi og brukervennlighet basert på studentenes erfaring. Verktøyene er delt inn i enkle verktøy (svart sirkel) og avanserte søkeverktøy (blå sirkel)

Når det gjelder avanserte søkemotorer, er «Verktøykassen» betydelig større. **Shodan**[14] er en nyttig søkemotor etter «Internet of things» (IoT) enheter. Shodan sender forespørsel til alle enheter koblet til internett daglig. Responsen den får – informasjon om porter, protokoller og eventuelle meldinger – lagres og presenteres sammen med eventuelle tekniske sårbarheter. Shodan-søk kan gi informasjon som display-meldinger, hardvare, programvare, internettleverandør, eier m.m. Shodan har også filtreringsmuligheter. Man kan filtrere på sted, IP-range, kategorier og portnumre blant annet. Shodan tilbyr å søke i en rekke portnummer som brukes i protokoller til spesifikke kontrollsystemer. Et eksempel er kommunikasjonsprotokollen DNP3. DNP3 ble konstruert med mål om å være pålitelig, men er ikke rustet mot digitale angrep. Protokollen brukes ofte i kraft- og vannbransjen, mellom SCADA og «Remote Terminal Unit» (RTU).

Maltego[15] er et OSINT-verktøy som automatiserer betydelige deler av den tidskrevende rekognoseringsprosessen. Maltego er en programvare som leverer og visualiserer informasjon i et lenket grafformat. Maltego kan lenke alt fra profiler på sosiale medier, e-postadresser og telefonnumre, til IP-adresser, steder og passord-lekkasjer. Andre avanserte søkemotorer er **Censys**[16]**, Nmap**[17] og **Foca**[18]**.** Censys og Nmap jobber på samme måte som Shodan. Fullversjonen av Censys er vesentlig dyrere en Shodan, og Shodan fremstår mer brukervennlig. Nmap krever god IT-kompetanse for å beherske da den har en tendens til å gi svært mye ekstra informasjon. Foca er et verktøy som brukes hovedsakelig til å finne metadata i skannede dokumenter og bilder. Slik metadata kan være forfattere, lokasjoner og datoer.



Figur 3 : Flytskjema over steg to i en intern revisjonsprosess.

Studentenes helhetlige vurdering av verktøyenes brukervennlighet og nytteverdi er illustrert i figur 2.

LinkedIn[19] er et sosialt nettverk som brukes i forretningsøyemed. LinkedIn er en god kilde for å finne ansattinformasjon og annen informasjon om et nettselskap.

CVE Details[20] er en søkbar sårbarhetsbase hvor man kan filtrere på produkter, leverandører, versjoner og kjente sårbarheter. Databasen oppdateres kontinuerlig.

SKISSE TIL REVISJONSPROSESS

De nevnte verktøyene kan brukes av virksomheten selv til å finne svakheter og sårbarheter for system og personer.

Første steg i en intern revisjonsprosess vil være å undersøke hva som ligger åpent om virksomheten som har opphav fra virksomheten selv, dens ansatte eller leverandører. Dette innebærer blant annet hjemmesider og sosiale medier. Dette regnes som «lavthengende frukt» da slik informasjon er lett å fjerne. Deretter undersøker man informasjon fra annet opphav. Til slike «overflatesøk» er Google Dorks nyttig. Relevante filtyper er pdf, pptx og xls, og domener som kan være virksomheten selv, leverandører

13 *https://doffin.no/*
14 *https://www.shodan.io/*
15 *https://www.paterva.com/*
16 *https://censys.io/*
17 *https://nmap.org/*
18 *https://www.elevenpaths.com/labstools/foca/index.html*
19 *https://www.linkedin.com/*
20 *https://www.cvedetails.com/*

eller dokumentarkiver som Docplayer[21] og Issuu[22]. Man kan også ta stikkprøver av viktige ansatte for å undersøke om vedkommendes jobb-e-postadresse finnes tilgjengelig på nett, og om den har vært utsatt for nylige passordlekkasjer. **Andre steg** i en intern revisjonsprosess vil være å etterligne en ekstern kartlegging av eget nettverk. Steget er forklart i flytskjemaet i figur 3. Via søkemotoren Shodan kan man søke på hele virksomhetens IP-range. For hver enhet som Shodan finner bør man vurdere om enheten behøver å være koblet til internett. Dersom man ikke kobler den fra, bør man videre vurdere om den er godt nok sikret. Vurderes sikkerheten som god nok kan man likevel vurdere å «skjule» enheten bak en brannmur eller VPN. Vurderes sikkerheten som ikke god nok, eller det finnes sårbarheter med enheten på CVE Details, må man undersøke om leverandøren tilbyr oppdateringer, eller legge til ekstra sikkerhet. For ytterligere undersøkelser bør alle IP-adresser undersøkes i Maltego, hvor de videre kan gi informasjon om personer, steder eller andre IP-adresser enheten kommuniserer med.

FUNN - STORT NETTSELSKAP

- Driftssentralsystem og leverandør.
- Ansatt som på LinkedIn oppgir SCADA på driftssentral som arbeidsrolle.
- Dokument som inneholder 51 ansatte i sentrale stillinger med navn, avdeling, rolle og jobb-e-post. Dokumentet avslører også e-post format.

FUNN - MELLOMSTORT NETTSELSKAP

- Flere bilder av driftssentral i media. Bildene avslører hvem og hvor mange som jobber der, hvilke områder overvåkningskameraene utenfor dekker, trådløs mus og tastatur fra leverandøren.
- Radiomottakeren står oppført med 14 sårbarheter på CVE details.
- PDF-presentasjon som sammen med datablad på leverandører sine produktoversikter gjør det mulig å kartlegge nesten fullstendige data- og kommunikasjonssystemer komponentvis.
- Bedriftens format på sine ansattes e-poster.
- IKT-konsulentens private e-post var utsatt for e-postlekkasje.
- Enlinjeskjemaer fra lokale områder, inkludert en klasse 1 transformatorstasjon.

FUNN - LITE NETTSELSKAP

- På nettsiden fant NVE oversikt over alle ansatte med fullt navn, stilling, jobb-e-post og telefonnummer.
- Virksomheten har ikke egen IT-avdeling, men får ekstern hjelp en gang i uken.
- 4 av 13 testede jobb-e-poster har vært utsatt for en datalekkasje inneholdende passord og annen personlig informasjon.
- Bilde som viser driftsleder på driftssentral.
- Nødnettradio – modell og frekvensområde.
- Hvor i bygningen sentralen er lokalisert.
- Leverandør og modell til kontrollsystem
- Enlinjeskjema tilknyttet vindpark og en klassifisert trafostasjon.
- Driftssentralrommet er ikke alltid bemannet.
- Overvåking og styring kan gjøres hjemmefra med bærbare PC-er.

ANBEFALING

NVE anbefaler at virksomhetene selv gjør en kartlegginga av virksomhetens «digitale fotavtrykk» og vurderer om noe informasjon på internett er sensitiv iht. kbf § 6-2 og bør fjernes; «*Med kraftsensitiv informasjon menes spesifikk og inngående opplysninger om kraftforsyningen som kan brukes til å skade anlegg, system eller annet eller påvirke funksjoner som har betydning for kraftforsyningen,…*».

NVE vil også anbefale virksomhetene å lære opp ansatte i grunnleggende IKT-sikkerhet, samt utvikle en god sikkerhetskultur. En start kan være å arrangere et sikkerhetsseminar for å bevisstgjøre hvordan ansattes og virksomhetens eksponering på internett påvirker risikoen.

Noen enkle tiltak som reduserer risikoen: Endre standardpassord og beskytt godt egne passord, ta i bruk flerfaktor-autentisering, ikke legg ut lister av ansattes eposter, vurder om komponenter må være synlige på internett og praktiser fotoforbud på viktige anlegg.

NVE vil minne om energilovens forpliktelse (ENL §9-3) til å beskytte kraftsensitiv informasjon, plikten gjelder enhver som får tilgang til eller behandler denne type informasjon

KONTAKT

For spørsmål kontakt beredskapsseksjonen, NVE.

[21] *https://docplayer.me/*

[22] *https://issuu.com/*