NASJONAL
SIKKERHETSMYNDIGHET

Informasjon om cyberrisiko for maritim sektor

Nasjonal sikkerhetsmyndighet (NSM) håndterer og koordinerer sikkerhetshendelser i cyberrommet knyttet til nasjonale interesser. Nasjonalt cybersikkerhetssenter (NCSC) ved NSM følger og analyserer situasjonsbildet døgnkontinuerlig og støtter utsatte virksomheter.

NSM NCSC har siden juni mottatt informasjon om kampanjer mot en rekke sektorer. Hendelsene har hatt et globalt omfang, men USA, Europa og Midtøsten skiller seg ut som fokusområder. Trusselaktørene har vist høy evne og vilje. Det er observert forsøk på digitale aksjoner mot enkelte virksomheter.

Basert på informasjonsgrunnlaget som foreligger, vurderer NSM NCSC at maritim sektor og olje- og gassektoren over det siste året har vært mål for målrettede kampanjer. Virksomheter må være forberedt på at aktiviteten kan fortsette på kort til mellomlang sikt.

Kampanjene kan ramme både åpenbare og mindre åpenbare virksomheter. I maritim sektor vurderer NSM NCSC, Norges rederiforbund og Sjøfartsdirektoratet at alle typer skip og rederienes landbaserte infrastruktur kan være sårbare for cyberhendelser. Virksomheter som opererer i MARSEC nivå 2-områder eller høyere bør være spesielt på vakt.

NSM NCSC oppfordrer virksomheter og ansatte i maritim sektor til å utvise økt årvåkenhet, og følge tiltakene i vedlegg 1. Mistenkelige hendelser bør rapporteres til Sjøfartsdirektoratet og Norges rederiforbund. Send en kopi av henvendelsen til NSM NCSC dersom det mistenkes at hendelsen skyldes aktivitet som beskrevet i vedlegg 2 eller annen form for cyberaktivitet. NSM NCSC kan kontaktes hele døgnet på telefon 02497 og e-post norcert@cert.no.

Med vennlig hilsen,

Nasjonalt cybersikkerhetssenter

**Informasjonen er offentlig tilgjengelig, kan publiseres og spres til publikum*

NASJONAL SIKKERHETSMYNDIGHET

Vedlegg 1: Anbefalte tiltak

På generelt grunnlag anbefaler NSM alle virksomheter å følge NSMs grunnprinsipper for IKT-sikkerhet[1] og veiledninger om bruk av sosiale medier [2,3].

Virksomheter oppfordres til å benytte seg av NSM NCSC varslingsliste. Påmelding kan sendes til post@cert.no.

Virksomheter kan be om teknisk kartlegging av egen sikkerhetstilstand gjennom NSMs tjeneste Allvis NOR. Allvis NOR[4] gjennomfører tekniske sårbarhetsundersøkelser av utvalgte tjenester som virksomheten melder inn. Tjenestene må være eksponert mot Internett. Interesse rettes til pentest@nsm.stat.no.

Basert på det aktuelle risikobildet anbefaler NSM NCSC følgende tiltak:

For virksomheter som har ansvar for infrastruktur på skip:

- Segmentering av nettverk. Det bør aldri være en fysisk forbindelse mellom administrative og operasjonelle nettverk.
- Loggfør aktivitet på endepunkter og i nettverket. NSM NCSC anbefaler å lagre loggene i minst 6 måneder.
- Benytt kryptert kommunikasjon så langt som mulig, også mellom skip og landbasert infrastruktur. Kommunikasjon kan enklere manipuleres når den er sendt ukryptert.
- Begrens tilgang til informasjon og systemer etter tjenstlig behov. Tilgangsstyring begrenser i mange hendelser konsekvensen av kompromitteringer.

Alle virksomheter med tilknytning til nasjonale interesser, eller som forvalter risikoutsatte verdier, anbefales å gjennomføre kontinuerlig sikkerhetsovervåking. Dersom virksomheten ikke har egen kapasitet kan NSMs kvalitetsordning for hendelseshåndtering benyttes[5].

Den enkelte bør være kritisk til lenker og vedlegg i e-postmeldinger:

- Er det tvil om vedlegg eller en lenker bør åpnes - vurder om det er strengt nødvendig. Rapporter mistenkelige meldinger, som kan knyttes til arbeidsstedet, til arbeidsgiver.
- Vær forsiktig med dokumenter som ber om å aktivere makroer i Word, Excel eller PowerPoint.

I sosiale medier for den enkelte:

- Mistenkelige meldinger mottatt på sosiale medier bør rapporteres til arbeidsgiver dersom de kan knyttes til arbeidsstedet.
- Etabler og vedlikehold kontakt kun med mennesker der identitet kan bekreftes.
- Vær kritisk til lenker og vedlegg i meldinger på sosiale medier.
- Forvent at alle kan se informasjonen som deles på sosiale medier, både om jobb og privatliv.
- Legg ikke ut arbeidsrelatert informasjon uten tillatelse fra arbeidsgiver.
- Legg ikke ut informasjon om andre uten deres tillatelse.
- Benytt sikkerhetsinnstillingene som er tilgjengelige i benyttede tjenester.
- Ikke bruk samme passord på tvers av tjenester.

[1] https://www.nsm.stat.no/globalassets/dokumenter/nsm_grunnprinsipper_for_ikt-2018.pdf
[2] https://www.nsm.stat.no/globalassets/dokumenter/brosjyrer/socialmedia_web.pdf
[3] https://www.nsm.stat.no/blogg/podcast---some-og-sikkerhet/
[4] https://www.nsm.stat.no/om-nsm/tjenester/sikker-kommunikasjon/allvis-nor/
[5] https://www.nsm.stat.no/om-nsm/tjenester/leverandorforhold/kvalitetsordning-for-bruk-av-leverandorer-av-tjenester-innen-ikt-hendelseshandtering/

Vedlegg 2: Observerte kampanjer

Følgende kampanjer er i den siste perioden observert av NSM NCSC.

Bruk av sosiale medier

I en kampanje har en trusselaktør benyttet LinkedIn for å sende skadevare etter at man hadde godkjent en forespørsel. Dette er en typisk fremgangsmåte som NSM NCSC også tidligere har observert. LinkedIn er en plattform som er enkel å utnytte for kartlegging av nøkkelpersonell og for leveranse av skadevare. Et eksempel på en slik kampanje kan leses i en artikkel fra cybersikkerhetsselskapet FireEye[6].

Når en kontakt godkjenner en LinkedIn-forespørsel, vil personen bak forespørselen, dersom det ikke er gjort endringer i standardinnstillingene, få tilgang til hele kontaktlisten. Denne listen kan igjen benyttes for å sende invitasjoner til andre LinkedIn-brukere. Informasjon fra forskjellige profiler kan benyttes til å beskrive personlige og jobbrelaterte interesser, arbeidssted, alder, rolle, kontaktinformasjon som e-postadresser og telefonnumre, utdanning, kurs, sikkerhetsklareringer, bilder, meninger, politisk tilhørighet, familieknytninger, med mer.

En enkeltperson trenger ikke å direkte oppgi jobbtilhørighet på LinkedIn for at en trusselaktør skal kunne utlede sensitiv informasjon fra profilen. Har aktøren tilgang til flere profiler, kan slik kunnskap utledes for å videre bygge en detaljert profil som i neste steg kan brukes i menneskelige eller teknologibaserte etterretningsoperasjoner. Dette leder til slutt til en høyere eksponering av sårbarheter hos enkeltpersonen og virksomheten.

E-poster med link eller vedlegg som kan installere skadevare

En annen kampanje som nylig er observert benytter e-postmelding som utgir seg for å komme fra kjente selskaper. Det kan være virksomheter eller enkeltpersoner, eller meldinger med vedlegg som ser ut som en vanlig faktura. I noen tilfeller vil disse føre til at det installeres skadevare på maskinen hvis en lenke eller vedlegg åpnes. I andre tilfeller er aktørene ute etter å kartlegge enkeltpersoner.

E-postene kan være vanskelige å skille fra vanlig søppelpost. Vi anbefaler derfor å utvise forsiktighet ved åpning av e-poster fra ukjente personer, spesielt dersom de inneholder linker eller vedlegg. I flere e-postklienter vil det være mulig å holde musepekeren over linken for å se om den peker til den faktiske linken som oppgis, eller undersøke om e-posten faktisk er sendt fra avsenderen. Aktørene baserer seg ofte på nye sårbarheter i systemer, og det anbefales derfor at man til enhver tid etterstreber å ha den nyeste versjonen av programmer og operativsystemer installert.

[6] https://www.fireeye.com/blog/threat-research/2019/07/hard-pass-declining-apt34-invite-to-join-their-professional-network.html