DIGITALT SITUASJONSBILDE

Kommune-CSIRT

Rapport nr. 1 – 2022

Rapporten er Kommune-CSIRT(K-CSIRT) sin beskrivelse og vurdering/analyse av digitale trusler, sårbarheter og hendelser i kommunal og fylkeskommunal sektor. Perioden for analysen er desember 2021 til april 2022.

Sammendrag

24. februar vil være en dato vi vil huske i lang tid. I denne utgaven vil vi vie hele delen om «Situasjonsbilde og vurderinger» til situasjonen i Ukraina, og hvordan krigen ikke bare foregår på bakken med også i cyberdomenet. K-CSIRT fremmer sin vurdering av situasjonen og tiltak som er viktige på nåværende tidspunkt for kommuner og fylkeskommuner.

Om man ser på krigen i cyberdomenet vil man kunne si at situasjonen har gjort aktørbildet enda mer uoversiktlig enn hva det har vært tidligere. Aktører som tidligere har bestått av både ukrainere og russere er nå blitt delt og kjemper en kamp mot hverandre. I tillegg er det mobilisert en rekke aktører utenfor Ukraina og Russland som kjemper hovedsakelig på Ukrainsk side. Med aktiviteten i cyberdomenet følger det også med nye skadevare. Det er observert flere typer såkalte «wipere», som er en type skadevare som ødelegger lagringsmedia for datamaskiner. Den første og mest kjente av disse skadevarene – kalt «HermeticWiper», ble antagelig testet ut allerede i november i Litauen hvor den ble observert. Denne typen skadevare kan være svært effektive som en saboterende faktor i en hektisk krigssituasjon med lite tilgang til ressurser for å ta hånd om slike angrep.

Vår vurdering så langt er at trusselbildet har endret seg, men ikke nødvendigvis mye til det verre for en gjennomsnitts norsk kommune- eller fylkeskommune. Bortsett fra enkelteksempler på phishing mot europeiske flyktningemyndigheter og noen angrep som har skadet både Ukraina og andre land, har den nye typen cyberoperasjonene i Ukraina ikke truffet Vest-Europa eller Norge i noen særlig grad. Likevel, på grunn av økt spionasje fra russisk etterretning (ref. de hemmelige tjenestenes trusselbilde) og et mindre forutsigbart aktørbilde i en dynamisk krigssituasjon, anbefales det økt årvåkenhet for alle. Myndighetene ber spesielt om årvåkenhet rundt kritisk infrastruktur og tjenesteløsninger for vannforsyning og helse, fordi det alltid er en mulighet for at statssponsede aktører angriper disse. Den vurderingen slutter vi oss til.

I forkant at krigens utbrudd i Ukraina sto verden ovenfor sårbarheten Log4Shell. Nasjonal sikkerhetsmyndighet sitt Cyber sikkerhetssenter NCSC meddelte 10. desember og gjennom dagen 11. desember at det var observert omfattende utnyttelsesforsøk av sårbarheten, og fått rapporter om tilsvarende fra samarbeidspartnere nasjonalt og internasjonalt. Sårbarheten ble vurdert som særlig kritisk da den i prinsippet berørte alt som var integrert mot og logges av Log4j, hvilket omfatter et stort antall utbredte tjenester.

I perioden har det også vært en rekke virksomheter som har vært utsatt for løsepengeangrep. Her kan det nevnes selskaper som Nordic Choice. Glamox, CGM, Nortura og Amedia. Det har også være flere, og fellesnevneren for ofrene er store utfordringer med å opprettholde normal drift og betydelige kostnader for å komme tilbake til normalsituasjonen. Dette viser at selv om vi følger med på situasjonen i Ukraina, må vi ikke glemme det vi har hatt fokus på i de foregående Situasjonsbildene. I perioden har det også være en rekke andre typer cyberangrep, dessverre rammet dette blant annet en norsk fylkeskommune.

Ut fra trusselbildet advarer vi i tiden som kommer mot de samme truslene som dette situasjonsbildet tar for seg. Det er viktig å følge situasjonen i Ukraina og tilhørende situasjon i cyberdomenet nøye. I tillegg tror vi på fortsatt phishing- og såkalt smishingkampanjer som er populærnavnet på SMS phishing. Dette gjelder fortsatt i april 2022. Tema helse vil antagelig bli benyttet videre og i tillegg vil vi se kampanjer rundt innsamling til humanitære ofre (denne gangen Ukraina), skatteetaten og skattemelding.

Hendelser

Nordic Choice Hotels rammet av løsepengevirus
2. desember ble Nordic Choice Hotells rammet av datavirus. Hotellene måtte bruke manuelle løsninger siden viruset rammet systemene for booking, innsjekk, utsjekk og betalingsløsningene. Kjeden gikk ut 6. desember med informasjon om at det var usikkerhet rundt om det var personopplysninger på avveie. De kunne også fortelle om at viruset var av typen løsepengevirus og at det var Conti som sto bak. 13. desember påtok Conti seg ansvaret for angrepet og publiserte 47 GB data fra Nordic Choice hotells.

Brudd på informasjonssikkerheten i dansk kommune
7. desember ble det kjent at en USB-pinne med data om over 92.000 innbyggere i Vejle kommune i Danmark var sporløst borte. Minnepinnen forsvant i forbindelse med kommunevalget den 16. november, skrev TVSyd.

Falske e-poster som angivelig kommer fra HelseNorge
8. desember ble det gjennomført en phishingkampanje hvor tjenesten HelseNorge ble misbrukt. Falske e-poster som inneholdt en lenke til en falsk nettside ble sendt ut. Ved å klikke på lenken ble man sendt inn på en falsk nettside som etterlignet innloggingssiden til IDporten. Norsk Helsenett skrev i en pressemelding at de falske e-postene var et forsøk på å svindle til seg informasjon som kunne bli brukt til økonomisk vinning. Norsk helsenett la til at HelseNorge aldri vil be om kredittkortinformasjon og sikkerhetskoder via tekstmelding eller e-post.

Bekjempelse av gigantisk sikkerhetshull
9. desember bla sårbarheten Log4Shell kjent. Nasjonal sikkerhetsmyndighet sitt Cyber sikkerhetssenter NCSC meddelte at de 10. desember og gjennom dagen 11. desember hadde observert omfattende utnyttelsesforsøk av sårbarheten gjennom VDI, og fått rapporter om tilsvarende fra samarbeidspartnere nasjonalt og internasjonalt. Sårbarheten ble vurdert som særlig kritisk da den i prinsippet berørte alt som var integrert mot og logges av Log4j, hvilket omfatter et stort antall utbredte tjenester. Til NTB sa Adam Myers, Datasikkerhetsekspert i Crowdstrike – Internett står i brann. Sårbarheten, døpt «Log4Shell», ble rangert til ti av ti på skalaen til Apache Software Foundation, som håndterer programvaren. Mens sikkerhetsfolk jobbet på spreng for å tette sikkerhetshullet, hadde datakriminelle allerede utviklet og distribuert verktøy for å utnytte sårbarheten. På verdensbasis hadde mange millioner servere verktøyet installert.

Glamox angrepet av samme trusselaktør som hacket Nordic Choice
10. desember ble det gjennom Digi.no kjent av belysningsleverandøren Glamox fra Molde nylig hadde blitt angrepet av Conti. Conti er en gruppe kjent for å kreve løsepenger via datainnbrudd, kryptovirus og trusler om å publisere stjålne data, skriver Digi.no. Konsernsjef Martinussen i Glamox uttalte 10. desember at det var blitt avverget et alvorlig dataangrep og at ingen filer hadde blitt kryptert. Konsernet skal heller ikke har mottatt noe krav om løsepenger. Dog ville ikke Martinussen ut fra artikkelen på digi.no utelukke at data kunne være på avveie.

Dataangrep mot Volvo
10.desember offentliggjorde bilprodusenten Volvo at de hadde vært utsatt for et dataangrep. Dette skal ha resultert i at data kom på avveie, skriver selskapet selv i en pressemelding, gjengitt i ZDNet. Undersøkelser som ble gjort kunne bekrefte at en begrenset mengde av selskapet data innen forskning og utvikling ble stjålet under innbruddet.

CGM – offer for løsepengeangrep
Mandag 20. desember ble CGM offer for løsepengeangrep. Firmaet leverer blant annet systemer for journalføring for leger og helsestasjoner i Norge. Angrepet var av typen «ransomware» og bestod i at en rekke filer i CGM sitt interne nettverk ble kryptert, skrev CGMN på egne nettsider. Alle servere og klienter tilknyttet CGM sine nettverk ble umiddelbart skrudd av, for å begrense spredningen. CGM uttalte videre at angrepet rammet kun CGM sine interne systemer. Eksterne systemer, som for eksempel tjenester over Norsk Helsenett (oppdatering, fjernstyring m.m.) eller deres driftsmiljøer for kunder (CGM Hosting) ble ikke rammet. Rutinemessig ble alle servere slått av og isolert for å begrense skade og forhindre ytterligere angrep. Ingenting tydet på at kundedata var ført ut av CGM sitt nettverk eller at kundeopplysninger ble påvirket av angrepet.

Nortura utsatt for dataangrep
21. desember ble Nortura utsatt for dataangrep. Etter oppdagelse av mistenkelig aktivitet på servere besluttet de raskt å stenge ned sine IT-systemer og fjerne internettilgangen på sine lokasjoner for å minimere mulig skade på systemer og operasjoner. Prioriteringen til Nortura ble å kontrollere sikkerhetshendelsen og produksjonsstøtte. Selv om Nortura var offline over en periode, ble det arbeidet med å skape mest mulig funksjonalitet i denne situasjonen.

Cyberangrep mot Nordland Fylkeskommune
27. desember kunne vi på digi.no lese at Nordland fylkeskommune (NFK) var blitt utsatt for datainnbrudd. Innbruddet ble oppdaget lille juleaften, og første konsekvens ble nedstengte nettsider for fylkeskommunen. Tidlig kunne NFK fortelle at de ikke hadde indikasjoner på at sensitiv informasjon var på avveie. Da alarmen gikk ble all internett-tilgang sperret, og de fikk etter hvert en god oversikt og ble rimelig sikre på hvordan angriperne kom inn. Mye tyder også på at NFK fikk stengt ned systemene før noe informasjon ble hentet ut.

Amedia - Utsatt for dataangrep
Natt til tirsdag 28. desember ble flere av Amedias sentrale datasystemer satt ut at drift. Produksjonen av nettavis ble ikke påvirket, mens det var full stans i produksjon av papiravis. En pressemelding utdypet at systemer for publisering av papiravis, annonser og abonnementshåndtering ikke fungerte som normalt. Etter hvert ble det klart at angrepsform og modus viste et klassisk løsepengeangrep der Amedia ikke var et spesifikt eller planlagt mål.

Cyberangrep på Ukrainske offentlig nettsteder og utplassering av skadevare
14. januar ble mer enn 70 offentlig nettsteder i Ukraina utsatt for dataangrep. Ondsinnet skadelig programvare som løsepengevirus ble oppdaget på flere datasystemer i etterkant av angrepet. Angrep mot myndigheters nettsider ble gjort for å skjule arbeidet med utplassering av skadelig programvare. ComputerWeekley.com skriver 17. januar: «*Kiev hevder at en hackergruppe i Hviterussland – en nær alliert av Russland – var ansvarlig for å hacke ukrainske myndigheters nettsteder midt i truslene om en militæraksjon».* Hackergruppen benyttet flere teknikker for å bryte seg inn i statlige datasystemer, inkludert et ukrainsk IT-selskap for å starte et "forsyningskjede"-angrep mot sine offentlige kunder.

Cyberangrep mot leverandør av tjenester til Røde Kors – Over 515.000 mennesker rammet
19. januar ble det kjent at et cyberangrep mot en leverandør til Røde Kors (kontraktor) hadde ført til tyveri av personopplysninger for mer enn 515.000 mennesker som tilhørte et «Restoring Family Links program». Programmet hjelper å gjenforene familier som er adskilt av krig, katastrofer og migrasjon. En kunngjøring kom fra den Internasjonale Røde Kors-komiteen (ICRC), som kunne opplyse at dataene ble samlet av minst 60 forskjellige nasjonale Røde Kors- og Røde Halvmåne-foreninger over hele verden.

Stor norsk vindu- og dørprodusent utsatt for løsepengevirus
21. januar ble det kjent at NorDan nylig hadde vært utsatt for at dataangrep. NorDan er en norsk produsent av vindu og dører. Angriperne hadde fått tak i påloggingsinformasjon til en konto og lyktes derfor med å komme seg på innsiden av IT-infrastrukturen. Der kunne de laste ned og stjele data, før de slapp løs et løsepengevirus som lammet IT-systemene. Tross angrepet klarte den norske milliardbedriften å opprettholde produksjonen i Norge, Sverige og Polen. Selv om produksjonen ble opprettholdt i stor grad, kostet angrepet virksomheten flere millioner kroner.

Securitas hacket, 3 TB med data knyttet til flyplassansatte på avveier.
7. februar ble det kjent at Securitas hadde blitt utsatt for et dataangrep. En usikret AWS-server med åpning mot det offentlige Internett var hovedårsaken til en kompromittering av data fra flyplassansatte i Colombia og Peru. Denne serveren tilhørte, ifølge en rapport fra SafetyDetectives, Securitas, et Stockholm-basert multinasjonalt selskap som blant annet tilbyr sikkerhetstjenester som sikkerhetsvakt, brann og sikkerhet og risikostyring i forsyningskjeden.

Invasjonen av Ukraina
Russiske styrker angrep tidlig på dagen 24. februar flere mål i Ukraina med krysserraketter og helikopter. Russiske styrker krysset grensen direkte fra russisk territorium, fra de okkuperte områdene Krim, Luhansk og Donetsk og fra hviterussisk territorium. Russland har også skutt mot Ukraina fra fartøyer i Svartehavet. Det russiske angrepet er det mest omfattende i Europa siden andre verdenskrig. Luftrommet over Ukraina ble stengt for sivil luftfart straks det var klart at angrepet var i gang. En rekke land iverksatte i løpet av få dager omfattende sanksjoner mot Russland. Det digitale domenet har vært en viktig del av krigen, også merkbart i opptakten til krigen – fra begynnelsen av januar til krigsutbruddet.

Angrepet på Viasat's satellittkommunikasjon
24. februar ble det gjennomført et cyberangrep som rammet den amerikanske satellittkommunikasjonsleverandøren Viasat. Hendelsen utløste brudd på satellitt-tjenestene over hele Sentral- og Øst-Europa og var sannsynligvis et resultat av en ødeleggende wiper-skadevare. Angrepet som også koblet fra ekstern tilgang til 5800 vindturbiner i Tyskland, ble først antatt å være et resultat av et distribuert tjenestenektangrep, men forskere som har sett nærme på angrepet tror det stammer fra wiper-skadevaren AcidRain som ble designet for å fjernslette sårbare modemer og rutere.

Phishing-kampanje rettet mot europeiske tjenestemenn som bistår i flyktningeoperasjoner
Sikkerhetsfirmaet Proofpoint ga 1. mars ut en rapport som viste til en phishing-kampanje med mulige koblinger til en statsstøttet aktør. Kampanjen var rettet mot europeiske tjenestemenn som støttet arbeidet med å evakuere ukrainske flyktninger. Selskapet skriver at attribusjon forble noe uklar på dette tidspunktet, men de fant likheter med kampanjer utført av nettspionasjegruppen kjent som UNC1151 (også referert til som GhostWriter eller TA445). Gruppen antas å være en hviterussisk statsstøttet aktør som støtter Russland i invasjonen av Ukraina.

Lapsus$-hackere lekket 37 GB av det de hevdet er Microsofts kildekode
22. mars skrev BleepingComputer at Microsoft ble oppgitt som det siste store selskapet som skal ha blitt offer for Lapsus$' herjinger. Gruppen hevdet 20. mars at de hadde stjålet kildekode fra Microsofts søkemotor Bing, taleassistenten Cortana og andre interne Microsoft-prosjekter fra en server, og postet skjermdumper som skulle bekrefte dette. Skjermgrafikkselskapet NVIDIA skal også ha blitt kompromittert av Lapsus$.

Situasjonsbilde og vurderinger:

Den 'normale' perioden - fra desember til januar

Desember er som regel en perfekt måned for cyberangrep. Gang på gang viser det seg at guarden er lavere under juleforberedelsene i landet vårt, både for personer og virksomheter. Slutten av 2021 fulgte i mønsteret og det ble en alvorlig bølge av avanserte angrep. Vi fikk kompromitteringer og løsepenge-angrep mot reiseliv, matproduksjon, media og kommunale skybaserte helseløsninger. Vi snakker da om rammede virksomheter som Nordic Choice Hotels, Nortura, Amedia og CGM (CGM journal, WinMed m.m.). En fylkeskommune ble også rammet, Nordland fylkeskommune. Uvedkommende kom seg inn i sentrale systemer og fikk en viss kontroll, men ble sannsynligvis stoppet før de fikk gjort mer skade - som for eksempel nedlåsing/kryptering av data. Dette nevnt som en mulighet, Kommune-CSIRT har ikke kjennskap til hva aktøren hadde som endelig mål.

Til tross for at det skjer en del arrestasjoner av kriminelle løsepengeaktører mot slutten av 2021 og i starten av 2022, fortsetter trenden med en strøm av nye aktører innen denne svært skadelige, kriminelle virksomheten. Utviklingen av denne trusselen støtter opp om vår vurdering fra tidligere Situasjonsbilder. Mot slutten av perioden som denne rapporten dekker, dukker det opp en del nye aktører og noe endret målretting. Mer om dette i neste avsnitt.

Konvensjonell krig og cyberkrig

24. februar 2022 går Russland til invasjonskrig mot Ukraina. Det var et sjokk for de fleste, og krigen har så langt medført umenneskelige lidelser og enorme ødeleggelser, samtidig som den forrykker det geopolitiske sikkerhetsbildet i Europa. Vår oppgave blir da å vurdere hvordan dette påvirker Norge og norske kommuner og fylkeskommuner når det gjelder digital sikkerhet.

Krigen føres ikke bare på land og i luften, men også ved hjelp av ulike cyberangrep fra begge sider. I denne cyberkrigen dukker det opp nye skadevarer, aktører og ofre. Når det gjelder skadevare, er det observert flere typer såkalte «wipere», som er en type skadevare som ødelegger lagringsmedia for datamaskiner. Det innebefatter både ødeleggelse av oppstartsområdet for operativsystemet («Boot record») og generell partisjonering/diskstruktur. Den første og mest kjente av disse skadevarene – kalt «HermeticWiper», ble antagelig testet ut allerede i november i Litauen hvor den ble observert. Slike wipere er normalt ikke kritiske så lenge man har tilgang på reservedeler, backup og IT-personell, og har god tid. Men som en saboterende faktor i en hektisk krigssituasjon med lite tilgang til de nevnte ressursene, kan denne typen skadevare være svært effektiv. Et observert eksempel er registrerings-PC-er ved grensestasjoner som ble sabotert av slik skadevare. Disse grensestasjonene hadde lange køer av flyktninger som skulle registreres. Uten IT-hjelp og backup måtte noen stasjoner gå over til penn og papir for registrering, og registreringskapasiteten ble sterkt redusert og køene økte. Denne skadevaren er etter det Kommune-CSIRT erfarer, kun observert i Ukraina, og hvor sannsynligheten er høy for at det er Russland som står bak. Den russiske trusselaktøren *Sandworm* antas også å stå bak nye wipere som Caddy Wiper og Industroyer2. Sikkerhetsselskapet ESET (Welivesecurity.com) og amerikanske myndigheter peker på den russiske militæretterretningsorganisasjonen GRU som de som styrer *Sandworm*. Slik skadevare er benyttet mot Ukraina tidligere, blant annet i angrep på Ukrainas kraftforsyning i 2016 og tidligere. Da også ble det pekt på statssponsede aktører fra Russland som ansvarlige.

Cyberkrigen startet allerede før den fysiske krigen brøt ut 24. februar. Det er logisk siden den russiske doktrinen for angrep på naboland legger stor vekt på cyberangrep og spionasje, både før og under en

fysisk krig. Utenom eksempelet fra Litauen, ble ukrainske regjeringsnettsteder angrepet og såkalt «defaced» (overtatt og plassert en melding på forsiden) i midten av januar, og flere angrep fulgte fram mot krigsutbruddet.

Figur 1 Cyberkrig-kartet (Kilde: Curated-Intel/Equinix)

Både Russland og Ukraina ser ut til å ha både kapasitet og ekspertise innen det vi kan kalle cyber warfare eller offensive cyberoperasjoner. Dette er også en informasjonskrig, og alle mulige kanaler blir brukt for å spre informasjon av begge parter – derunder mye falske kontoer og nyheter. Dermed rammes også sosiale medier i Russland - med blant annet myndighetenes sperring av FB og Instagram.

Ukraina har på sin side fått med seg en del aktivister som støtte – det beste eksempelet er gruppen Anonymous (Anon). Anon har lyktes i å ta ned både russiske medier og regjeringssider, samt nettsiden til det russiske romsenteret (IKI). Ukrainske myndigheter forsøker også å verve frivillige fra hele verden til sin «IT Army», og ser ut til å ha lykkes i noen grad.

En helt ny vri er at det har oppstått nye løsepengeaktører som nå angriper russiske nettsteder og virksomheter! Dette fenomenet har så å si vært ikke-eksisterende fram til krigsutbruddet. Nå har det dukket opp aktører som tar kontroll over .ru nettsteder og legger ut lekkede data på det mørke nettet. Se figur 2. Til og med en løsepengeaktør (Stormous) sitt nettsted på det mørke nettet (TOR), er hacket og nedlåst! Slike angrep mellom kriminelle har ikke vi observert tidligere.

Claimed Victim	Ransomware Gang	Detection Date (UTC+0)	Ransomware URL	Victim Site	Victim Country
panasonic	Conti	2022-04-05 09:11:36	Not supported to FREE version	www.panasonic.com	Canada
scoular.com	LockBit	2022-04-05 08:21:38	Not supported to FREE version	scoular.com	USA
Roskomnadzor	Anonymous	2022-04-05 05:52:48	Not supported to FREE version	rkn.gov.ru	Russia
Transneft	Anonymous	2022-04-05 05:52:48	Not supported to FREE version	transneft.ru	Russia
Rosatom	Anonymous	2022-04-05 05:52:48	Not supported to FREE version	www.rosatom.ru	Russia
Central Bank of Russia	Anonymous	2022-04-05 05:52:48	Not supported to FREE version	www.cbr.ru	Russia
Rostproekt	Anonymous	2022-04-05 05:52:48	Not supported to FREE version	rstpr.ru	Russia
MashOil	Anonymous	2022-04-05 05:52:48	Not supported to FREE version	mashoil.ru	Russia
Thozis Corp	Anonymous	2022-04-05 05:52:48	Not supported to FREE version	Unknown	Russia
Marathon Group	Anonymous	2022-04-05 05:52:48	Not supported to FREE version	marathongroup.ru	Russia
Capital Legal Services	Anonymous	2022-04-05 05:52:48	Not supported to FREE version	cls.ru	Russia
Mosekspertiza	Anonymous	2022-04-05 05:52:48	Not supported to FREE version	www.mosekspertiza.ru	Russia
petsk Mechanical Plant	Anonymous	2022-04-05 05:52:48	Not supported to FREE version	lmz48.ru	Russia
VGTRK	Anonymous	2022-04-05 05:52:48	Not supported to FREE version	vgtrk.ru	Russia
Korolevskiy	Anonymous	2022-04-05 05:52:48	Not supported to FREE version	korolevskiy.ru	Russia

Figur 2 Anonymous sin leak site på den mørke nettet viser russiske ofre (Kilde: Darktracer.com)

Løsepengeaktørene har også problemer med å velge side da mange tydeligvis har personell som holder med forskjellige sider i krigen. Dermed utløses splittelse, og den største aktøren av dem alle – Conti – har fått lekket enorme mengder interne dokumenter, veiledere, chatlogger osv. som er distribuert av gruppen som kaller seg @ContiLeaks. Til tross for mye interne stridigheter, fortsetter de kriminelle operasjonene nesten med uforminsket styrke og med nye aktører.

Det er verdt å merke seg at vestlige land og virksomheter jobber hardt for å støtte Ukraina i kampen mot digitale trusler. Den amerikanske regjeringen og FBI publiserte i begynnelsen av april at de har tatt ned sentrale deler av et botnet kalt Cyclops Blink. Botnettet bestod for det meste av tusenvis av WatchGuard Firebox brannmurer, og ble styrt av den russiske hackegruppen Sandworm eller Voodoo Bear. Denne gruppen antas å stå bak tidligere angrep på Ukrainas kraftnett og

bankvirksomhet i 2015 og 2016. I begynnelsen av april melder Microsoft at de har tatt ned syv domener som har blitt brukt i digitale angrep mot Ukraina av en annen GRU-tilknyttet hackergruppe – kalt APT28 eller Fancy Bear. Dette er positive tegn – det nytter å bekjempe også disse avanserte aktørene!

Det norske kommuner må være spesielt oppmerksomme på, er kontakter mot russiske og ukrainske selskaper, institusjoner, leverandører og annet internasjonalt samarbeid som involverer disse to. Slike kanaler kan bli misbrukt, temaer om humanitær hjelp kan brukes i phishing, og det er ikke sikkert at alt er det som det gir seg ut for å være. Det kan til og med gjelde flyktninger.

Vår vurdering så langt er at trusselbildet har endret seg, men ikke nødvendigvis mye til det verre for en gjennomsnitts norsk kommune- eller fylkeskommune. Bortsett fra enkelteksempler på phishing mot europeiske flyktningemyndigheter og noen angrep som skadet både Ukraina og andre land (eks. Viasat), har den nye typen cyberoperasjoner i Ukraina ikke truffet Vest-Europa eller Norge i noen særlig grad. Men både på grunn av økt spionasje fra russisk etterretning (ref. de hemmelige tjenestenes trusselbilde) og et mindre forutsigbart aktørbilde i en dynamisk krigssituasjon, anbefales det økt årvåkenhet for alle.

Myndighetene ber spesielt om årvåkenhet rundt kritisk infrastruktur og tjenesteløsninger for vannforsyning og helse, fordi det er alltid en mulighet for at statssponsede aktører angriper disse. Det slutter vi oss til.

Her er et sett med de viktigste tekniske og prosessmessige tiltakene som bør gjennomføres:

- Bruk multifaktor-autentisering for **all** tilgang utenfra **(inkl. leverandører)**
- Unngå aktivering av innhold i e-poster!
- Sørg for reell offline backup
- Fjern utrangert utstyr
- Vær oppdatert – sørg for et effektivt og raskt oppdaterings-/patcheregime
- Geofencing/sperring mot utlandet (i den grad det er mulig).

Glasskula – hva ser vi komme?

Siste utgave (desember 2021) advarte vi mot helserelatert phishing, og det slo til, også for såkalt smishing som er populærnavnet på SMS phishing. Dette gjelder fortsatt i april 2022, og tillegg har vi en strøm av de vanlige temaene rundt innsamling til humanitære ofre (denne gangen Ukraina), skatteetaten og skattemelding.

De siste månedene har vi observert noe som kan utvikle seg til en ny trend, en ny aktør som hacker store selskaper- de kaller seg Lapsus$ - stjeler store mengder data fra virksomhetene, og forsøker å presse disse for penger. Ikke noe nytt i det, men de krypterer altså ikke dataene, er veldig aktive på sosiale medier som Telegram hvor de henger ut sine ofre, og forsøker åpent å få ansatte i store konsern å lekke brukernavn og passord mot betaling. Ofrene er store, globale selskaper som NVIDIA, Microsoft, Samsung, Okta og Ubisoft. Betaling og annen oppfølging mot banden er visstnok ikke lett, så business-caset ser lite gjennomarbeidet ut. Det spekuleres i om dette er en gruppe som er ute etter berømmelse, heder og ære i miljøet, eller om de bare er ferske i gamet. Kommune-CSIRT vurderer det som å ha en viss sannsynlighet at slike bander vil øke i antall og at de vil iverksette alvorlige angrep mot norske kommuner og fylkeskommuner.

Kommune-CSIRT vurderer det som sannsynlig at statssponsede cyberoperasjoner vil angripe og forsøke å kompromittere kritisk infrastruktur i Norge i løpet av de neste 6-12 måneder. Konsekvenser kan være både lekket politisk, forskningsmessig og militær informasjon til fremmede makter, samt leveranseproblemer for energi og vann.

Siste side

Rapportens aktuelle situasjonstips:

Sikkerhetskultur og operasjonell sikkerhet:

- Ikke aktiver innhold i vedlegg og ikke klikk på lenker verken i epost eller SMS (uten å dobbeltsjekke med avsender)
- Ikke bruk jobbkonto til private formål
- Gjenbruk av brukernavn og passord er ingen god idé og må unngås!

De viktigste sikkerhetstiltakene:

- Sørg for multi-faktorautentisering for *all* tilgang utenfra
- Sørg for å ha sikkerhetskopier som er reelt offline, og testet for gjenoppretting
- Oppgrader alt internett-eksponert utstyr så raskt det lar seg gjøre - angrepene mot disse øker
- Ikke la utrangert utstyr bli stående eksponert mot internett

Relevante rapporter, dokumenter og kampanjer lansert i perioden:

Nasjonal sikkerhetsmyndighet – Risiko 2022: https://nsm.no/getfile.php/137798-1644424185/Filer/Dokumenter/Rapporter/NSM_rapport_final_online_enekeltsider.pdf

PST – Nasjonal trusselvurdering 2022: https://www.pst.no/alle-artikler/trusselvurderinger/ntv-2022/

Etterretningstjenestens åpne vurdering av aktuelle sikkerutfordringer for Norge – Fokus 2022: https://www.forsvaret.no/aktuelt-og-presse/publikasjoner/fokus/rapporter/Fokus-2022-til-web.pdf/_/attachment/inline/ec6bec00-d2d3-41c0-af08-02b3b494e8b7:e4014ab4d0e3bd8b2509e7974430fe121e0473ba/Fokus-2022-til-web.pdf

K-CSIRT ønsker å minne om viktige nasjonale prinsipper og strategier:

NSMs grunnprinsipper for IKT-sikkerhet:
https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/introduksjon-1/

Nasjonal strategi for digital sikkerhet:
https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/nasjonal-strategi-for-digital-sikkerhet.pdf

Tiltaksoversikt til Nasjonal Strategi for digital sikkerhet
https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/tiltaksoversikt---nasjonal-strategi-for-digital-sikkerhet.pdf

Kommune-CSIRT støtter sine medlemmer med råd, varsling og tiltak innenfor både strategisk og operativ informasjonssikkerhet. Vi støtter også medlemmene ved hendelser og fungerer som et bindeledd mellom tekniske hendelseshåndterere og virksomhetsledelse, og mellom ledelse og andre kommuner, sektorer og myndigheter. **Kontakt Kommune-CSIRT: post@kommunecsirt.no eller telefon 90 85 00 42.**