DIGITALT SITUASJONSBILDE

Kommune-CSIRT

Rapport nr. 2 – 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 april 2022 til oktober 2022.

Sammendrag

Sist vi lanserte vårt situasjonsbilde var vurderingen at trusselbildet hadde endret seg, men ikke nødvendigvis til det verre for norske kommuner. En måned senere advarte vi mot hevnaksjoner utført av pro-russiske grupper som KillNet og Legion. Dette slo dessverre til. Vi ble kjent med at en rekke virksomheter som Skatteetaten, BankID og Stortinget ble rammet. Dette var såkalte distribuerte tjenestenektangrep (DDoS) som ble utført med den konsekvens at eksterne tjenester fra virksomhetene blir utilgjengelige over korte eller litt lenger perioder. Selv om slike angrep ikke er så alvorlige i seg selv og ikke påfører varige skader, kan det i verste fall - etter lang tids angrep - medføre svekket tillit til de viktigste digitale tjenestene våre. Angrepene mot norske tjenester viser også at den politiske ledelsen i Russland har støtte blant aktivistgrupper som er i stand til å hevne seg direkte overfor land som støtter Ukraina med våpen eller foretar andre handlinger som blir oppfattet som anti-russisk. Oppblomstringen og utviklingen av denne type aktører peker mot flere og mer avanserte cyberangrep i de neste månedene – inkludert alvorlige kompromitteringer.

Sammenliknet med 2021 har 2022 så langt vært roligere når det gjelder alvorlige kompromitteringer og digital utpressing av norske virksomheter. Ute i Europa og resten av verden ser digital utpressing ut til å fortsette på samme intense nivå som tidligere. Vi kan nevne angrep mot italienske kommuner, Creos i Luxembourg og South Staffordshire Water i Storbritannia. Begge sistnevnte er teknisk infrastruktur-operatører.

I 2016 kom det en stor bølge innover Norge av en svindeltype som ble kalt «Direktørsvindel hvor e-post ble sendt i direktørens navn til en økonomiansatt for å få gjennomført en utbetaling til svindlerne. Denne typen svindel har det vært forskjellige arter av som har gått i bølger siden den gang. Den siste tiden har vi hørt om flere tilfeller av denne typen svindelforsøk. Phishing pågår hele tiden og ansatte lærer gjennom e-læring hva de skal se etter når en e-post kan være mistenkelig. Derimot kan det bli større utfordringer å hanskes med svindelforsøk som er mer målrettet og til og med blir utført fra en overtatt/kompromittert e-postkonto. Vi kan i denne utgaven rapportere om forsøk på direktørsvindel mot både en kommune og en fylkeskommune. Et av forsøkene ble gjennomført fra en overtatt/kompromittert kommunal brukerkonto mot en ansatt, mens fylkeskommunen ble utsatt for mer tradisjonell direktørsvindel og fikk i alt om lag 80 svindeleposter tilsendt til ansatte i løpet av 7 dager.

Våre vurderinger av situasjonsbildet senere i rapporten favner denne gangen ganske bredt, men vi kommer ikke utenom situasjonen i Ukraina og hvordan dette påvirker cybersikkerheten hos oss. Norge har blitt en svært viktig leverandør av gass til kontinentet etter at leveransene fra Russland ble redusert, og sabotasjeaksjonen i Østersjøen og droneobservasjoner i Norge forsterker sannsynligheten for nye Cyberoperasjoner mot Norges kritiske leveranser og infrastruktur. Når kabler i havet mellom Norge og utlandet ifølge myndigheter og eksperter er utsatt, gjelder det selvsagt også digitale kabler og vår tilgang til internett.

Vi vil fortsatt se aksjoner som tjenestenektangrep og andre cyberangrep mot det offentlige Norge i tiden fremover, inkludert det som ligger innenfor kommunale ansvarsområder. I dette ligger også mulig skadeverk og sabotasje på kritisk operasjonsteknologi og kommunikasjonsnettverk som eies av eller er viktig for norske kommuner og fylkeskommuner. Kommune-CSIRT vurderer i denne uoversiktlige situasjonen trusselnivået og risikoen for høyere enn ved forrige rapport i april.

Hendelser

Rumenske myndigheter rammet av KillNet
Rumenske myndigheters nettsteder ble 29. april rammet av den russiske hackergruppen KillNet. Den rumenske regjeringen uttaler fredag 29. april at de har opplevd nettangrep fra en russisk kilde. Nettsteder som tilhører offentlige institusjoner, inkludert regjeringen og forsvarsdepartementet, ble rammet av tjenestenektangrep, som startet klokken 04.00 lokal tid og antas å ha sin opprinnelse i Russland. Den russiske hackergruppen KillNet tok på seg ansvaret, ifølge rumenske regjeringskilder.

Microsoft advarer mot russiske statssponsede hackere
I uke 17 uttalte Microsofts visepresident Tom Burt at selskapets eksperter tror cyberangrep vil fortsette å eskalere ettersom krigen mellom Russland og Ukraina fortsetter.
"Russiske nasjonalstats-trusselaktører kan få i oppgave å utvide sine destruktive handlinger utenfor Ukraina for å gjengjelde de landene som bestemmer seg for å gi mer militær bistand til Ukraina og ta flere straffetiltak mot den russiske regjeringen som svar på den fortsatte aggresjonen," sa Burt.
"Vi har observert russisk-vennlige aktører som er aktive i Ukraina, viser interesse for eller gjennomfører operasjoner mot organisasjoner i Baltikum og Tyrkia - alle NATOs medlemsland som aktivt gir politisk, humanitær eller militær støtte til Ukraina."

Datainnbrudd hos Norkart – persondata på avveie
10. mai ble det kjent at persondata for opp til 3,3 millioner nordmenn kan være stjålet. Uvedkommende utnyttet en sårbarhet/feilkonfigurering i brannmuren til søketjenesten som henter kopidata fra Norges offisielle eiendomsregister. Eiendomsregisteret har oversikt over hvem som eier hva i Norge. Fortrolige adresser og skjermede bygg ble ikke berørt av datainnbruddet. De fleste av opplysningene det her er snakk om kan man finne andre steder på internett, bortsett fra personnummer. Det som er spesielt her er at opplysningene er samlet på ett sted.

Hacking av Italias forsvarsdepartement og senat
11. mai kunne vi lese at nettsteder som tilhører Italias forsvarsdepartement og senat blant flere, var rammet av en hackergruppe, som også tok på seg ansvaret for et nylig nettangrep på tyske myndigheters nettsteder. Aktivistiske hackere (også kalt *Hacktivister*) har i økende grad rettet seg mot vestlige institusjoner siden krigen i Ukraina startet. En pro-russisk hackergruppe kjent som "KillNet" sto bak nettangrep på nettsteder som tilhører flere italienske institusjoner, rapporterte Italias nyhetsbyrå ANSA. På kvelden den 11. mai fungerte ikke nettsteder som tilhører Italias forsvarsdepartement, Senatet og National Health Institute. Politiet var tidlig ute og fortalte at etterforskning pågår, men ga ingen ytterligere detaljer. Før KillNet rettet seg mot Italia, har de også gått målrettet mot offentlige og private selskaper i andre land, inkludert USA, Estland, Latvia, Tyskland, Polen, Tsjekkia, Ukraina og Romania som nevnt. Nettstedene de retter seg mot indikerer at angripernes mål inkluderer land som støtter Ukraina eller på annen måte fremstår som motstandere av Russland.

Forsøk på hacking/angrep på Eurovision
14. mai ble finalen i Eurovision Song Contest 2022 avholdt i Italia. I en rekke medier kunne man dagene etter lese om at både Eurovision-finalen og de to tidligere semifinalene hadde blitt utsatt for målrettet tjenestenektangrep (DDoS) av den pro-russiske hackergruppen KillNet, heter det i en uttalelse fra det italienske politiet. Forsøkene ble blokkert. Konkurransen, som ble holdt i Italia, ble sett på som en offentlig demonstrasjon av solidaritet med Ukraina og en utstrømning av anti-krigsfølelse over hele Europa, med Russland utestengt fra Eurovision tidligere på året. I et Telegram-innlegg slo KillNet tilbake mot de italienske myndighetenes påstander og sa at de ikke sto bak angrepet.

Den toneangivende trusselaktøren Conti har lagt ned driften under eget navn
I mai ble det rapportert om at den beryktede Conti ransomware-gjengen offisielt har lagt ned driften, med infrastruktur tatt offline og teamledere som har fortalt at «varemerket» ikke lenger eksisterer. Samtidig har det forekommet betydelige lekkasjer fra Contis virksomhet, blant annet er store deler av chat-loggene lekket, analysert og publisert. Dette har gitt sikkerhetsanalytikere god informasjon om hvordan den største aktøren innen digital utpressing har operert. Mens Conti varemerket ikke er mer, vil cyberkriminalitetssyndikatet fortsette å spille en betydelig rolle i løsepengevareindustrien i lang tid fremover, blant annet som underleverandører og mulig oppdeling og rebranding til nye grupper.

Russiske hackere sto bak Nortura-hacking
Nortura melder 23. mai at hackerangrepet mot selskapet i desember 2021 ble gjennomført av russiske hackere. Selve cyberangrepet ble gjennomført 21. desember. Nortura stengte ned sine interne IT-systemer og fjernet internettilgangen på flere av sine driftssteder. Først 3. januar gjenopptok selskapet driften ved hjelp av midlertidige løsninger for å ta igjen arbeidet som måtte utsettes i jula. Oslo-politiet har etterforsket dataangrepet med bistand fra Kripos.

Personopplysninger lå åpent tilgjengelig i Rogaland fylkes nettsky
Tidlig i juni ble det meldt om at elevvurderinger, barnevernsmeldinger og en omfattende adresseliste lå åpent tilgjengelig i nettskyløsningen til Rogaland fylkeskommune. Skyløsningen var knyttet til Microsoft365, som fylkeskommunen bruker for elever og ansatte. Stavanger Aftenblad som først meldte om saken har sett dokumentasjon på opplysninger som søkbare og tilgjengelige i en felles mappe, blant annet bekymringsmeldinger til barnevernet om elevers atferd og mulig rusbruk. Også elevvurderinger og en liste med navn, adresse og personnummer til nesten 3500 mennesker var tilgjengelig.
Fylkeskommunen var ikke kjent med datalekkasjen da Stavanger Aftenblad tok kontakt, men stengte adgangen etter noen minutter. «Vi har meldt avvik internt og melder avvik til Datatilsynet», sier fylkeskommunens sjef for digital utvikling, Svein Vathne til Digi.no. Han sier sakene er veldig uheldige.

Flere bølger med DDoS-angrep mot norske myndigheter og virksomheter
Fra 29. juni og i begynnelsen av juli ble flere sentrale norske samfunnsinstitusjoner og medier som NSM, NRK, DN, VG, Altinn, Arbeidstilsynet, Skatteetaten, BankID og Politiet rammet av DDoS-angrep (tjenestenektangrep). Pro-russiske KillNet som Kommune-CSIRT advarte mot i mai, har påtatt seg skylden for angrepene. Dette er samme gruppe som stod bak tidligere nevnte angrep mot Italia, Romania og Eurovision. DDoS eller tjenestenektangrep består av å sende en overflod av datatrafikk mot en internett-eksponert tjeneste, som for eksempel en nettside, slik at tjenesten blir ustabil eller utilgjengelig.

Finsk nyhetsbyrå hacket
30. juli melder den statlige kringkastingen YLE om at nyhetsbyrået STT er tatt av hackere, og noen av systemene deres ble tatt offline dagen før (fredag 29.7). Det er ikke uvanlig at hackere går mot medieorganisasjoner. Som vi har varslet om tidligere ble det norske medieselskapet Amedia utsatt for et cyberangrep som stengte datasystemene deres, og hindret utgivelsen av aviser i papirformat.
Panu Tuunala, STTs administrerende redaktør, sa at byrået nå hadde økt beredskapen for å håndtere potensielle cyberangrep. Han sa samtidig at det fortsatt var uklart hvem som var ansvarlig for angrepet og om hackerne stjal data. Senere har den russiske activistgruppen NoName057(16) tatt på seg ansvaret for angrepet.

Creos gassrørleding i Luxembourg tatt av BlackCat/ALPHV
1. august kunne vi lese om at gassrørledningsoperatøren Creos og morselskapet Encevo i Luxembourg kjempet mot et angivelig løsepengevareangrep som startet uken før, den siste i en rekke hendelser som involverer europeiske energiselskaper. Hackingen skjedde antagelig 22.7. Selskapet skrev at angrepet tok ned kundeportaler for begge selskapene, men at det ikke påvirket forsyningen av elektrisitet og gass.

Dette fremstod som å kunne være hevnmotiv mot Europa. Banden antas å være en rebranding av Darkside som ble BlackMatter og som igjen ble BlackCat/ALPHV/. Darkside ble vurdert å være russisk/pro-russisk, og man kan anta at det også gjelder rebrandede grupper.

Hackere angrep britisk vannforsyning, men presset feil virksomhet
South Staffordshire Water, et selskap som leverer 330 millioner liter drikkevann til 1,6 millioner forbrukere daglig utstedte en uttalelse som bekreftet brudd på IT-systemene etter et nettangrep. Kunngjøringen forklarte at sikkerhets- og vanndistribusjonssystemene fortsatt var i drift, så forstyrrelsen av IT-systemene påvirket ikke forsyningen av trygt vann til kundene eller datterselskapene til Cambridge Water og South Staffs Water. Mens arbeidet pågikk hos de nevnte virksomhetene fremmet Clop løsepengevaregjengen Thames Water som sitt offer via en kunngjøring på deres nettside på det mørke nettet, med påstand om å ha tilgang til SCADA-systemer (styringssystemer for industrielle prosesser) de kunne manipulere for å skade 15 millioner kunder. Thames gikk ut og sa at de gjennomførte full operasjonell drift uten problemer, og etter at forhandlinger mellom offeret og Clop gikk i stå, ble deler av data fra hendelsen publisert.
Blant de publiserte bevisene presenterte Clop et regneark med brukernavn og passord, som inneholdt South Staff Water og South Staffordshire e-postadresser. Det er svært sannsynlig at Clop feilidentifiserte offeret sitt eller at de forsøkte å presse et mye større selskap ved å bruke falske bevis.

Montenegro utsatt for massive nettangrep; Russland er gitt skylden
Det koordinerte angrepet startet rundt 20. august og lammet offentlig drevne transporttjenester og nettbaserte plattformer for informasjon, samt vann- og elektrisitetssystemer. Etter første bølge av angrep har Montenegro vært utsatt for en serie organiserte cyberangrep på regjeringens IT-infrastruktur. Det primære målet er strukturen til statlig myndigheter. Maras Dukaj (Minister of administration) sa at IT-systemer ikke ble permanent skadet og benektet at noen data ble stjålet under angrepet. Flere kraftselskaper ble tvunget til å gå tilbake til manuelle prosesser etter angrepet, ifølge Reuters. Situasjonen er beskrevet på følgende måte på nbcnews.com «*Ved regjeringshovedkvarteret i NATO-medlemmet Montenegro er datamaskinene koblet fra, internett er slått av og statens hovednettsteder er nede. Blackouten kommer midt i et massivt nettangrep mot den lille Balkan-staten. Myndighetene sier at angrepet bærer preg av pro-russiske hackere og dets sikkerhetstjenester».* Den russiskvennlige ransomware-operatøren Cuba har påtatt seg ansvaret for deler av angrepet.

Stortinget ble rammet av DDoS-angrep 23. august.

Natt til tirsdag 23. august ble Stortingets nettsted, stortinget.no, utsatt for et distribuert tjenestenektangrep (DDoS-angrep). Ifølge uttalelse gitt til VG medførte dette ekstra belastning mot Stortingets systemer. I etterkant av angrepet opplevde Stortinget nettverksforstyrrelser uten at de knyttet dette til det foregående angrepet. IT-sjefen i Stortingets administrasjon hevdet at dette trolig kom av driftsfeil.

Forsøk på svindel mot en norsk kommune
Kommune-CSIRT ble varslet om at en kommune hadde fått kompromittert en brukerkonto. Tilgang til kontoen ble benyttet til å gjennomføre svindelforsøk mot en annen ansatt i kommunen. Dette var et målrettet forsøk på direktørsvindel som startet via en phishing-link 25. august. Angriperne gjemte seg bak anerkjente tjenester i MS Azure. Der ble man sendt videre til en *Evil-proxy* (teknikk for å hacke seg forbi 2-faktorautentisering) hvor «session token» (midlertidig innloggingsbevis) ble tatt. Angriperen satte opp en egen autentiseringsmekanisme for den kompromitterte kontoen rett før angrepet ble avdekket og passordet resatt. Den kompromitterte kontoen ble benyttet til å sende e-post fra CEO til CFO. Angriperen hadde kontroll på kommunikasjon mellom de to ved en videresendingsregel på CEO sin konto som sendte e-post fra CFO til en RSS feed og videre til angriperne. Kjente metoder som spearphishing og whaling ble brukt. Innloggingsbeviset («Session token») ble tatt 25. august. Deretter var det stille til 30. august hvor

resten av handlingene ble utført. Angriper har ikke lykkes å logge på kontoen etter denne datoen. Metodene som ble brukt vil sannsynligvis bli sett oftere framover.

Fylkeskommune utsatt for omfattende forsøk på Direktørsvindel
Fredag 9. september ble Kommune-CSIRT varslet fra en fylkeskommune om et forsøk på svindel av typen «Direktørsvindel/CEO-fraud». Et eksempel på en e-post er som følger: "Hei XXX, Er du tilgjengelig? det er en hastebetaling jeg må du gjøre på mine vegne. Gi meg beskjed slik at jeg kan sende deg detaljene. Hilsen xxx". I tilfellene fylkeskommunen har vært utsatt for har «avsendernavn» vært skrevet korrekt i mailene. Derimot har det ikke vært tvil om at dette er svindelforsøk om man har sett avsenders e-postadresser. En utfordring med disse svindelforsøkene er om mottaker leser e-post på telefon. Da vil ikke avsenders e-postadresse vises om du ikke spesifikt går inn i e-posten for å se på den. Totalt har fylkeskommunen sett ca. 80 forsøk på denne typen svindel mot ansatte i egne organisasjoner i løpet av en tidsperiode på 7 dager. Forsøkene på svindel har vist seg å treffe svært bredt. I starten var det økonomimedarbeidere, deretter toppledere og til slutt så man svindelforsøk mot ansatte langt ut organisasjonen, eksempelvis rektorer og ansatte ved skoler.

Europeiske kommuner kompromittert av ransomware
I juli ble åtte kommuner i Toscana-distriktet i Italia ofre for et ransomwareangrep som medførte nedetid på mange tjenester i flere dager. Kommunene hadde et IT-samarbeid under navnet «Unione di Comune Valdiseve e Valdarno». Trusselaktøren RansomHouse ble sagt å stå bak angrepet. Sent i september ble den portugisiske kommunen De Loures (geografisk beliggende i stor-Lisboa-området), tatt av ransomware-aktøren Hive. Den 5. oktober ble den italienske kommunen Rosignano Marittimo i Toscana tatt av ransomware. Kommunen uttalte at de oppdaget hendelsen tidlig, koblet seg fra internett og hadde offline-backup som gjorde dem i stand til å komme raskt tilbake i drift. Dette er noen eksempler, det finnes mange tilsvarende hendelser i Europa de siste månedene.

Situasjonsbilde og vurderinger:

Pro-russiske grupper og hevnaksjoner
I april var vår vurdering at trusselbildet har endret seg, men ikke nødvendigvis til det verre for norske kommuner. I foredrag i mai måned advarte vi mot hevnaksjoner utført av pro-russiske grupper som KillNet og Legion. Dette slo dessverre til – både i mai, juni og nå sist mot Stortinget i august. De siste angrepene tar hactivist-gruppen NoName057(16) på seg ansvaret for som kommunisert gjennom sin Telegram-kanal. Dette var såkalte distribuerte tjenestenektangrep (DDoS) som fører til at eksterne tjenester fra virksomhetene blir utilgjengelige korte eller litt lenger perioder. Men det blir ikke påført varige fysiske skader, lekkasjer eller nedlåsinger. Alt dreier seg om å overbelaste tjenestene for å gjøre dem utilgjengelige. Selv om disse angrepene ikke er ødeleggende i seg selv og ikke påfører varige skader, kan det i verste fall - etter lang tids angrep - medføre svekket tillit til de viktigste digitale tjenestene våre.

Angrepene mot norske tjenester viser også at den politiske ledelsen i Russland har støtte blant aktivistiske grupper som er i stand til å hevne seg direkte overfor land som støtter Ukraina med våpen eller foretar andre handlinger som blir oppfattet som anti-russisk, for eksempel problemene med frakt av forsyninger til Svalbard via Finnmark. Oppblomstringen og utviklingen av denne typen aktører peker mot flere og mer avanserte cyberangrep i de neste månedene – inkludert alvorlige kompromitteringer.

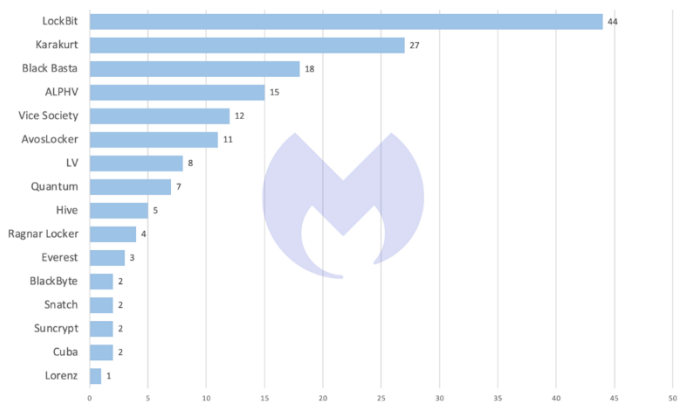
I flere utsagn og rapporter fra vestlig etterretning de siste årene hevdes det at det er forbindelse mellom russisk cybercrime-grupper og statlig etterretning – at de i noen grad samarbeider om skadevare og sårbarheter. Hvis de i tillegg samordner og koordinerer felles angrep for at deler av angrepet ikke skal oppdages, er det en farlig kombinasjon. Vi har noen indikasjoner på slikt tett samarbeid. Vår vurdering er at dette foreløpig ikke representerer en stor risiko i seg selv, men situasjonen kan raskt endre seg.

Det vestlig etterretning derimot har observert over flere år, er ulike grupperinger innenfor militær etterretning som har hatt ulike oppgaver innenfor en kampanje. En gruppe er 'bråkete', den er lett å oppdage og fungerer som en avledningsmanøver. Den andre jobber mer i det skjulte med blant annet informasjonsuthenting/spionasje.

Sabotasje i Østersjøen
Mandag 26. september ble det utløst flere undersjøiske eksplosjoner i Østersjøen ved gassrørledningene NordStream 1 og 2. Rørledningene går mellom Russland og Tyskland og eies i hovedsak av russiske Gazprom (hhv 51 % og 100 %). Eksplosjonene som skjedde nær den danske øya Bornholm, medførte store gasslekkasjer siden gassen stod under trykk i rørene. Selve leveransene har ikke vært operative siden august, da disse ble stoppet på grunn av krigen (NordStream 1). NordStream 2 har aldri vært i operativ drift. Kommentatorer og politikere er enige om at dette er bevisste handlinger og at det dermed klassifiseres som sabotasje. Russland skylder på USA, og de fleste i Vesten mener det er Russland som har mest å vinne på sabotasjen og er den aktøren som sannsynligvis står bak.

Figur 1: Illustrasjon NordStream-sabotasje (Kilde: Aftenposten)

Sammenliknet med 2021 har 2022 så langt vært roligere når det gjelder alvorlige kompromitteringer og digital utpressing av norske virksomheter. Samtidig har vi siden mai opplevd mange hevnaksjoner mot sentrale tjenester fra russiske aktivister. Ute i Europa og resten av verden ser digital utpressing ut til å fortsette på samme intense nivå, jamfør antall bedrifter utsatt for såkalt dobbel digital utpressing (med lekket informasjon på det mørke nettet) i grafikken fra sikkerhetsselskapet *Malwarebytes*.



Figur 2: Antall kompromitteringer juni 2022 (Kilde: Malwarebytes)

Som eksempel observerer vi at åtte italienske kommuner ble tatt av aktøren *RansomHouse* i slutten juli, og det engelske vannforsyningsselskapet South Staffordshire UK ble kompromittert i august av den kriminelle gruppen *Clop*. Sistnevnte aktør har uttalt at de spesialiserer seg på tekniske installasjoner og vannverk. Angrepet på statlige institusjoner og infrastruktur i Montenegro bør også nevnes, da angrepet pågikk i mange uker og mange tjenester ble satt ut av spill – inkludert kraftleveranser. Angrepet ble sett i sammenheng med at den montenegrinske presidenten var på besøk i Ukraina for å uttrykke sin støtte. Ytterligere eksempler finnes på at kommuner og statlige virksomheter er blitt tatt av ransomware i perioden juli til september.

Vurderinger og anbefalinger

Ut fra både reelle angrep på norske kommuner den siste tiden, og utviklingen av cyberkriminalitet og spionasje/sabotasje, er vår vurdering at utviklingen ikke peker entydig i en retning. Én hypotese kan være at norske offentlige virksomheter i mindre grad enn andre betaler de kriminelle og at de jevnt over har fått bedre sikkerhet. En annen forklaring kan være at dette er en midlertidig pause og at norske kommuner og virksomheter vil oppleve en ny bølge nærmere jul. Inngangen til julehøytiden har nesten uten unntak vært tiden for cyberangrep mot norske virksomheter, vi kan nevne Norsk Hydro, Østre Toten kommune, Nordland fylkeskommune, Choice Hotel og Nortura som alle ble kompromittert rett før jul.

Sabotasjen i Østersjøen viser at det er økt fare for angrep mot undersjøisk energiproduksjon og -eksport. Observasjoner av ukjente droner rundt plattformer i Nordsjøen, kraftstasjoner og forsvarsanlegg bidrar til å styrke vurderingen om økt farenivå. Og når først kabler i havet mellom Norge og kontinentet (og UK) er utsatt, gjelder det selvsagt også digitale kabler og vår tilgang til internett.

Som NSM tydelig viser i sin aktuelle og informative rapport *Nasjonalt digitalt risikobilde 2022*, har Russland benyttet cyberangrep mot Ukrainsk kritisk infrastruktur i lang tid. I rapporten beskrives en tidslinje med angrep datert fra mai 2014 til diverse angrep etter krigsutbruddet 24. februar i år. Den nylige selektive bombingen mot vann- og strømforsyning i Ukraina (oktober-22) understreker kritikaliteten og sårbarheten i et lands tekniske infrastruktur og -leveranser.

Den alvorligste trusselen mot norske og dermed også kommunale interesser, er mulige angrep på olje- og gass-sektoren. Norge har blitt en svært viktig leverandør av gass til kontinentet etter at leveransene fra Russland er sterkt redusert. All informasjon om anlegg, prosesser og teknisk styring er svært interessant for trusselaktører, og kan avdekke sårbarheter som kan muliggjøre sabotasje ved hjelp av cyberangrep. Vår erfaring er at digitale angrepsforsøk foregår kontinuerlig mot alle internetteksponerte tjenester og teknisk infrastruktur er intet unntak. Sikkerheten må forbedres for å redusere denne risikoen.

Alle kommuner som har kraftproduksjon eller -transport i sine områder, må være ekstra på vakt. Digitale angrep mot tekniske installasjoner i Norge kan også innbefatte kommunal VA og andre kommunaltekniske løsninger. Her trengs det både skippertak og kontinuerlige forbedringsprosesser for å øke sikkerheten, og Kommune-CSIRT jobber med dette området hver dag.

Etter sommerferien har Kommune-CSIRT fått en økning av rapporter om såkalte *direktørsvindelforsøk* mot norske kommuner og fylkeskommuner. Om dette skyldes bedret/økt rapportering eller en faktisk økning er usikkert, men vår vurdering er at denne typen cyberangrep fortsatt er meget aktuell. Vi anbefaler norske kommuner og fylkeskommuner om å være ekstra på vakt mot phishing og hasteutbetalingsønsker sendt elektronisk, da denne aktiviteten ikke har minket i omfang og blir stadig mer sofistikert.

Totalt sett er det digitale situasjonsbildet forverret siden vår siste rapport. Angrep fra og kildematerialet rundt russiske hactivist-grupper gir grunn til bekymring. Det er grunn til å anta at de oppildnes og støttes av sine myndigheter til stadig flere og mer alvorlige angrep på Ukrainas støttespillere. Trusselen fra statssponsede trusselaktører for spionasje og sabotasje er også stigende. Vi lever i en omskiftelig og uoversiktlig situasjon, både når det gjelder trussel- og risikobilde. Et noe lavere aktivitetsnivå mot Norge fra avanserte kriminelle de siste månedene kan likevel vurderes som positivt – samtidig som det kan være bare en midlertidig pause.

Glasskula – hva ser vi komme?

I høstmånedene ser vi fram mot julehøytiden og gleder oss til litt fritid og samvær med familie og venner. Jula og tiden like før er også en aktiv periode for kriminelle bander i det digitale domenet. Hvert år gjentar *forfalsket pakkesporing og andre phishing-kampanjer* seg – nærmest til det kjedsommelige. Det vil også skje i år – i et omfang og profesjonalitet som vil nå nye høyder – det er vår spådom. Aktuelle hendelser og tema som for eksempel Ukraina-krigen, strømpriser, vaksinasjon og gasseksport, vil som tidligere bli benyttet som tematisk blikkfang og lokkemat.

Vi er naturlig nok enda mer opptatt av de mer avanserte aktørene som i lang tid forbereder og gjennomfører cyberangrep mot kommuner, fylkeskommuner og andre offentlige virksomheter i Norge. For de neste 3-6 måneder advarer vi spesielt mot *digitale og hybride angrep mot norsk energiproduksjon, -transport og -eksport* og alt som hører med av digitale styrings- og informasjonssystemer.

Siden vi nå – basert på hendelsen i Østersjøen og meldinger om økt droneaktivert i Norge - kan forvente økt aktivitet fra utenlandsk etterretning og mulige sabotasjeaksjoner, bør også all kritisk infrastruktur i norske kommuner og fylkeskommuner sikres ekstra godt. Vår vurdering er at det sannsynligvis vil forekomme forsøk på både digitale *sabotasjeaksjoner, utpressing og spionasje* mot norske kommuner det neste halvåret. Noen av disse vil dessverre også lykkes.

Vi har en truende og uoversiktlig situasjon, og det kan være mange grunner til at antallet vellykkede, alvorlige angrep mot norske kommuner har en viss nedadgående tendens de siste månedene. Det er derfor ingen grunn til å trappe ned den gode jobben med å trygge norske kommuner.

Siste side

Rapportens aktuelle situasjonstips:

Sikkerhetskultur og operasjonell sikkerhet – for vanlige brukere:

- Ikke aktiver innhold i vedlegg og ikke klikk på lenker verken i epost eller SMS (uten å dobbeltsjekke med avsender)
- Aktiver multifaktorautentisering der du kan.
- Gjenbruk av brukernavn og passord er ingen god idé og må unngås!

De viktigste sikkerhetstiltakene – for drifts- og sikkerhetsavdelingen:

- Sørg for multifaktorautentisering 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
- Gjennomfør ekstra sikkerhetssjekk på tekniske installasjoner, VA og SD-anlegg.

Relevante rapporter, dokumenter og kampanjer lansert i perioden:

Nasjonal sikkerhetsmyndighet – Nasjonalt digitalt risikobilde 2022:https://nsm.no/getfile.php/1312007-1664785983/NSM/Filer/Dokumenter/Rapporter/NDIG2022_online.pdf

Nasjonal sikkerhetsmyndighet – E-læringskurs i NSMs grunnprinsipper for IKT-sikkerhet
Gratis e-læringskurs gjennom oktober: https://nsm.no/aktuelt/tilbyr-populart-sikkerhetskurs-gratis

Næringslivets sikkerhetsråd – Mørketallsundersøkelsen 2022: https://www.nsr-org.no/aktuelt/morketallsundersokelsen-2022-er-na-tilgjengelig

Østre Toten kommune/NTNU – Rapport etter dataangrepet, Publisert 30.09.2022:
https://www.ototen.no/aktuelt/rapport-etter-dataangrepet.15279.aspx

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.**