DIGITALT SITUASJONSBILDE

Kommune-CSIRT

Rapport nr. 1 – 2023

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 september 2022 til februar 2023.

Sammendrag

2021 var et dystert år for digital sikkerhet i Norge, men også internasjonalt. Vi kan nevne hendelser som Østre Toten, Drammen VA, Colonial Pipeline, Kaseya, hacking av Stortingets epostserver, Volue, Nordland fylkeskommune, Nortura og Amedia. Vi var forberedt på at 2022 kunne bli like ille, og et nytt faremoment ble introdusert gjennom krigsutbruddet i Ukraina 24. februar.

Slik ble det ikke i Norge i 2022, i hvert fall ikke når det gjelder kommuner og andre offentlige virksomheter. Det er observert en klar nedgang i antall vellykkede angrep og kompromitteringer, selv om noen private selskaper i Norge har blitt rammet av digital utpressing den siste tiden. En av de mest alvorlige hendelsene i 2022 er etter vår vurdering Norkart sin sårbarhet/feilkonfigurering som medførte tyveri av opplysninger om 3 millioner eiendomsbesittere i Norge. Nevnes bør også tjenestenektangrepene mot viktige nasjonale tjenester/funksjoner som Altinn, Stortinget og Nasjonal sikkerhetsmyndighet (NSM). Mot slutten av fjoråret ble Rec Silicon og Stangeland Maskin tatt av ransomware/digital utpressing. Likevel peker analysen totalt sett mot en viss nedgang i antall vellykkede cyberangrep, særlig når det gjelder de mest alvorlige angrepene.

I resten av Europa har cyberangrepene tilsynelatende ikke avtatt i styrke. Mot slutten av fjoråret ble det rapportert om vellykkede cyberangrep mot kommuner, blant annet fra Sverige, Danmark Tyskland, Bulgaria, Nederland og Italia. Ellers har også cyberangrep rammet både nordiske myndigheter, media og næringsliv/industri.

I Norge har vi nå i starten av 2023 sett kompromittering av kommuner og digitale hevnaksjoner som har blitt gjennomført mot norske sykehus. Dette viser at faren utvilsomt er høy uansett om vi opplever roligere perioder. Dette styrker vurderingen av at angrepsvolum og alvorlighet går i bølger, og at risikoen derfor fremdeles er høy for å bli angrepet og kompromittert.

I flere av rapportene som er lansert de siste 2 årene har man kunnet se hendelser mot vann og avløpssystemer over hele verden. I denne rapportutgaven gis det god plass til temaet *«Operasjonsteknologi og digital prosesstyring i norske kommuner og fylkeskommuner».* Vannforsyning er definert som kritisk infrastruktur og Grunnleggende Nasjonal Funksjon (GNF). Styringen av vannforsyningen er digitalisert - nesten overalt. Digitaliseringen medfører at kontrollsystemene - av effektivitetshensyn - er gjort tilgjengelig via internett, noe som muliggjør styring, overvåking og kontroll fra nær sagt hvor som helst i verden. Denne tilgangen gjør styringen sårbar for cyberangrep, og det blir viktig å ha moderne og oppdaterte sikkerhetsmekanismer på plass for slik styring og overvåking.

Til slutt i rapporten ser vi igjen inn i glasskula. I vår analyse og utsikter for 2023 forventer vi fortsatt et høyt volum av digitale angrep. Både hevn-hacktivisme (jfr. hevnaksjoner mot nasjoner som støtter Ukraina, se «Situasjonsbilde og vurderinger»), sofistikert phishing, forsyningskjedeangrep (angrep via underleverandører, programvareleverandører eller IT-partnere) og kompromittering via eksponerte tjenester vil forekomme. Det samme gjelder kombinasjonsangrep hvor svindlere benytter både epost og telefon for å overbevise ofrene om å utføre uheldige handlinger som medfører svindel eller kompromittering.

Hendelser

Kommune på Grønland tatt av ransomware
15. oktober ble Kujalleq kommune på Grønland tatt av ransomware med sannsynlighet for data på avveie. Kommunen selv uttalte at Cyberangrepet dessverre medførte en stor risiko for at personopplysninger fra kommunens IT-systemer var blitt stjålet. Det fulle omfanget er ikke kjent.

Datainnbrudd Domeneshop
Domeneshop meldte mandag 17. oktober om et datainnbrudd og at kunders data var på avveie. Dataene skal inneholde e-postadresser til brukere, brukernavn, krypterte passord og beskrivelse av brukeren. I en driftsmelding skrev Domeneshop at selv om alle passord er kryptert, kan det være et spørsmål om tid før de vil kunne bli kompromittert.. Til Aftenposten uttalte styreleder i selskapet Dag Øien at flere hundre tusen passord kan være kompromittert. Domeneshop har over 100.000 kunder og 600.000 domener, opplyser selskapet på sine nettsider.

KillNett fortsetter sine kampanjer
18. oktober kunne vi lese om at Pro-russiske hackere sto bak et "storskala" nettangrep på bulgarske myndigheters nettsteder på lørdag 15. oktober. Det distribuerte tjenestenektangrepet (DDoS) tok i en kort tid ned nettsidene til presidentadministrasjonen, forsvarsdepartementet, innenriksdepartementet og justisdepartementet. Den pro-russiske hackergruppen KillNet tok på seg ansvaret for angrepet og sa at det var en straff «for svik mot Russland og levering av våpen til Ukraina».

DDOS/Tjenestenektangrep mot EU-parlamentet
23. November. Nettstedet til EU-parlamentet var nede i omtrent en time etter at en pro-russisk hackergruppe gjennomførte et målrettet distribuert tjenestenekt (DDoS)-angrep. Angrepet kom bare timer etter at EU-parlamentet utpekte Russland til statssponsor av terrorisme. Erklæringen hevdet at Russlands angrep på ukrainsk infrastruktur, skoler og sykehus brøt med internasjonale lover.

Ransomware-aktør trodde de hadde tatt en belgisk kommune – tok politiet
26. november kunne vi lese om at aktøren Ragnar Locker, en kjent ransomware-aktør, hadde publisert stjålne data fra det de trodde var Zwijndrecht kommune i Belgia. Dette viste seg i stedet å være stjålet fra Zwijndrecht-politiet, en lokal politienhet i Antwerpen, Belgia. De lekkede dataene avslørte angivelig tusenvis av bilnummerskilt, bøter, kriminalitetsrapportfiler, personelldetaljer, etterforskningsrapporter med mer.

Nettsted brukt for spoofing av telefonsamtaler tatt ned
28. november kunne vi lese at «iSpoof» som leverer en såkalt spoofing-tjeneste har blitt tatt ned etter en internasjonal politietterforskning. Dette førte til arrestasjoner av til sammen 146 personer, inkludert den mistenkte hjernen bak tjenesten. Over hundre av disse arrestasjonene, inkludert den av plattformens leder, ble foretatt av Londons Metropolitan Police.

Dataangrep og driftsforstyrrelser i svenske regioner
Flere svenske regioner ble tirsdag 6. Desember rammet av dataangrep og driftsforstyrrelser. Dette gjaldt blant annet regionen Sörmland og Västra Götaland. Västra Götaland fikk opp igjen sine systemer i løpet av formiddagen samme dag. I Region Sörmland var nettverksavbruddet mer omfattende og påvirket helse og omsorgstjenester. Timebestillinger måtte kanselleres, og noen av regionens virksomheter fikk begrenset kapasitet på grunn av feilen. Region Sörmland opplyste onsdag at feilen skyldtes en uheldig konfigurasjon av regionens datasystemer.

Antwerpen sine tjenester gikk ned, samarbeidspartner utsatt for cyberangrep
6. desember kunne vi lese at Antwerpen i Belgia jobbet med å få gjenopprettet sine digitale systemer etter et leverandørkjedeangrep mot Digipolis, byadministrasjonens partner og leverandør av administrativ programvare. Forstyrrelsen rammet tjenester som brukes av innbyggere, skoler, barnehager og politiet. Ifølge Het Laatste Nieuws (HLN) var hackerne i stand til å ramme Antwerpens tjenester etter å ha brutt seg inn i serverne til Digipolis.

To svenske kommuner rammet av cyberangrep
Tirsdag 13. desember ble det skrevet om at en "krisesituasjon" hadde blitt erklært i de svenske kommunene Borgholm og Mörbylånga etter at et cyberangrep ble oppdaget sent mandag. Det ble bekreftet et innbrudd i det felles IT-systemet som brukes av de to kommunene, som til sammen utgjør øya Öland med en samlet befolkning på i overkant av 25.000 innbyggere. Gjennom første natten etter at de oppdaget angrepet koblet IT-personellet begge distriktenes offisielle systemer fra internett som en forholdsregel, og «eksterne aktører» ble hentet inn som en del av kommunenes hendelseshåndteringsrespons, sa Borgholms kommunalsjef Jens Odevall. Senere analyser antyder at det var ransomware-aktøren Cuba som stod bak angrepet og at de hadde stjålet/eksfiltrert 85 GB med data. Angrepet ble stoppet før de kriminelle fikk startet kryptering av data.

Stangeland maskin rammet av dataangrep
Da ansatte hos Stangeland maskin kom på jobb 15. desember møtte de låste datasystemer og adgang til alle programmer var sperret. Selskapet hyret inn eksperter på datasikkerhet for å få kontroll på situasjonen. Politiet ble også informert. Ifølge Aftenbladet skal hackerne ha krevd flere titalls millioner kroner i løsepenger for å låse opp igjen datasystemene.

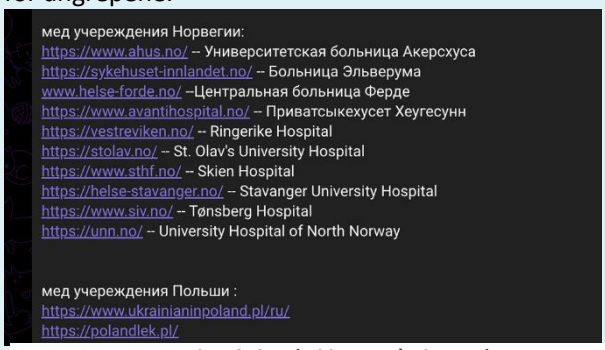
Rec Silicon rammet av digital utpressing/ransomware
19. desember: REC Silicon ASA ble rammet av et dataangrep. Selskapets virtuelle servermiljø ble rammet av et løsepenge-angrep som førte til at en rekke systemer sluttet å fungere for en kort periode. Selskapet engasjerte en virksomhet med kompetanse på hendelseshåndtering, og med spesialister på gjenoppretting av data, restaurering av systemer, utbedring og etterforskning. Alle systemer i selskapet ble gjenopprettet med bare mindre tap av data. Selskapets produksjon, sikkerhet, kvalitet, salg og regnskap var ikke påvirket av hendelsen. Selv om alle REC-systemer ble gjenopprettet, har beklageligvis trusselaktøren eksfiltrert (kopiert ut/stjålet) en begrenset mengde data som ikke ser ut til å inkludere noen vesentlige immaterielle rettigheter til selskapet.

TV2 utsatt for flere dataangrep
TV2 play ble torsdag 05. januar utsatt for et dataangrep. Angrepet førte til at 18000 kunder måtte bytte passord. Natt til fredag og fredag var TV2.no nede flere ganger. Pressesjef i TV2 uttalte til E24 at angriperne benyttet blant annet passord som er lekket på nettet for å logge seg inn på brukerkontoer. Brukere som har samme passord på forskjellige tjenester, kan derfor være rammet. For å beskytte TV2s kunder mot misbruk, ble alle berørte kontoer sperret og passord ble tilbakestilt. 18.000 kunder hos strømmetjenesten TV 2 Play måtte dermed bytte passord for å få adgang til tjenesten igjen

Det Norske Veritas utsatt for digital utpressing.
7. januar ble DNV utsatt for et vellykket angrep på sitt ShipManager-system. Selskapet bekrefter at de ble utsatt for digital utpressing/ransomware, og at serverne ble tatt ned for å håndtere hendelsen. Ingen andre DNV-tjenester var rammet og ShipManager-instansene om bord på skip fungerte fortsatt og ble ikke rammet, ifølge selskapet.

Norske sykehus angripes med tjenestenektangrep fra russiske hacktiviste

Lørdag 28. januar opplevde en rekke norske sykehus tjenestenektangrep fra russisk støttede hackere som hevn for Norges støtte til Ukraina. Denne typen angrep skaper midlertidig trengsel og tjenestebrudd på nettsidene til sykehusene, men gjør ingen skade på de interne funksjonene og systemene. Angrepene var varslet på forhånd, og det var den russiske gruppen som kaller seg KillNet som truet og påtok seg ansvaret for angrepene.



Figur 1: Angrepstruede sykehus (Kilde: NRK/Telegram)

Nordnorske kommuner kompromittert av hackere

I starten av februar 2023 kom det meldinger om at både Vadsø kommune og Målselv kommune har blitt hacket av ondsinnede aktører som har kompromittert e-postkontoer og servere. Det viser seg at angrepet mot Målselv var mot servere, mens Vadsø og andre kommuner og virksomheter har blitt kompromittert gjennom overtagelse av brukerkontoer/e-postkontoer. Det er foreløpig ingen indikasjon på at Målselv-hendelsen har tilknytning til hackingen av brukerkontoer hos Vadsø og de andre virksomhetene. Men Vadsø-hendelsen ser derimot ut til å gjelde flere kommuner og virksomheter, og denne hendelsen ser ut til å være større enn først antatt.

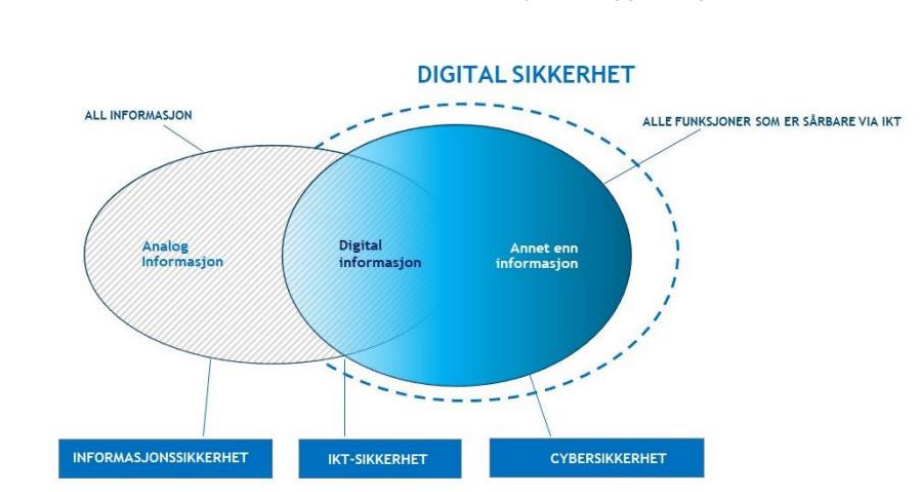
Situasjonsbilde og vurderinger:

TEMA: Operasjonsteknologi og digital prosesstyring i norske kommuner og fylkeskommuner

I vår kommunikasjon og vårt sikkerhetsarbeid snakker vi som oftest om informasjonssikkerhet og personvern. Våre oppgaver som CERT for kommunesektoren dekker imidlertid mer enn det. Vi tar også tak i sikkerhetsutfordringer hvor det ikke nødvendigvis er informasjon som skal beskyttes. Eksempler på dette er:

- digital prosesstyring av vannforsyning,
- SD-anlegg (systemer for sentral drifts av eks. varme og ventilasjon)
- låsesystemer for bygg
- idrettsanlegg
- velferdsteknologi
- heisstyring
- sikkerhetskameraer/overvåkingskameraer
- tuneller/veibommer
- kraftverk/kraftforsyning
- renseanlegg
- avfallsdeponi og forbrenningsanlegg

Et dekkende begrep for vårt fagområde blir derfor *digital sikkerhet* eller *cybersikkerhet*. Dette samsvarer med regjeringens definisjon fra strategidokumentet for digital sikkerhet fra 2019, og med modellen i figuren under som først ble publisert av NVE, og senere benyttet av Direktoratet for e-helse i sin strategirapport om digital sikkerhet fra 2020.



Figur 22: Digital sikkerhet (kilde: Direktorat for e-helse)

Figuren illustrerer at digital sikkerhet inneholder informasjonssikkerhet (digital sådan), men også mye mer, hvor dette heldekkende begrepet ofte forklares med «alle funksjoner som er sårbare via IKT». Digitaliseringen av tjenester brer om seg overalt i kommunesektoren, og derfor må også sikkerheten innenfor digitale kontrollsystemer ivaretas.

Krigsutbruddet i Ukraina 24. februar i fjor har medført forhøyet beredskap i mange sektorer i Norge, inkludert Forsvaret og energisektoren. Utøvd sabotasje på gassrørledninger i Østersjøen og mistenkelig aktivitet utført av russere – til vanns og på land – har ytterligere forsterket oppfordringen om økt

årvåkenhet og beskyttelse av kritisk infrastruktur. Dette har betydning for norske kommuner som har ansvaret for vannforsyningen til sine innbyggere. Vannforsyning er definert som kritisk infrastruktur og Grunnleggende Nasjonal Funksjon (GNF). Styringen av vannforsyningen er digitalisert - nesten overalt. Digitaliseringen medfører at kontrollsystemene - av effektivitetshensyn - er gjort tilgjengelig via internett, noe som muliggjør styring, overvåking og kontroll fra nær sagt hvor som helst i verden. Denne tilgangen gjør styringen sårbar for cyberangrep, og det blir viktig å ha moderne og oppdaterte sikkerhets-mekanismer på plass for slik styring og overvåking.

Operasjonsteknologi (OT) er et begrep som ofte brukes når man skal skille mellom generell IT og digitalisert prosesstyring. OT som inngår i et styrings- eller overvåkingssystem kalles på norsk driftskontrollsystemer (DKS), eller på engelsk *Industrial Control Systems* (ICS).

Kommune-CSIRT har hatt mange gjennomganger av digitale styringssystemer hos VA og andre tekniske systemer for våre medlemskommuner. Disse avdelingene er bemannet av dyktige ingeniører med høy spesialkompetanse og yrkesstolthet for sine etatsspesifikke oppgaver, og det med rette!

Samtidig har digitaliseringstakten vært høy også her, og den nye operasjonsteknologien og den digitale sikkerheten denne krever, er normalt ikke en del av de nevnte ingeniørenes utdannelse og fagområde.

Noen kriminelle trusselaktører har større fokus på DKS enn andre, og for eksempel Cl0p-banden hevder å jobbe målrettet mot vannforsyningssystemer. Hacktivistgruppen GhostSec hevder å ha lykkes i å kryptere en russisk RTU (Remote Terminal Unit) som er en type ruter for kommunikasjon mellom sentrale styringssystemer (SCADA) og perifert utstyr som igjen styrer for eksempel ventiler, sensorer og pumper. Faren for at norske kommuner skal bli utsatt for akkurat slike angrep, er relativt liten. I Norge benyttes det etter det vi har opplysninger om, annen teknologi og tilgangsmetoder enn i GhostSec-eksempelet. Våre metoder og teknologi sikrer ikke mot digital kompromittering av driftskontrollsystemer av den grunn. Det er mange andre metoder som kan bringe skadevare inn og infisere kritiske komponenter.

Basert på gjennomgangene av tekniske styringssystemer og vannforsyningssystemer hos våre medlemskommuner, er vår vurdering at den digitale sikkerheten behøver en grundig sjekk. Sikkerheten kan være mangelfull av flere årsaker:

- tilgangssystemer har lav sikkerhet, svake passord og kan enkelt hackes
- gamle, utdaterte systemer / mangelfullt patcheregime gjør systemene sårbare
- mangelfull sikkerhetskompetanse i den kommunale etaten
- mangelfull sikkerhetskompetanse hos leverandører
- manglende samhandling på sikkerhet mellom IT og teknisk/VA
- uklar/mangelfull rollefordeling og bruk av upersonlige brukerkontoer

Fylkeskommunene har ikke ansvar for vannforsyningen i fylket sitt, men de har både SD-anlegg, låsesystemer og andre typer OT som for eksempel tunnelovervåking i samarbeid med Statens vegvesen. Fylkene råder over mye eiendomsmasse – som eksempel har videregående skoler egne bygg eller lokaler. Det viser seg at disse byggenes SD-anlegg ofte er styrt av leverandører med tilgang utenfra som har ukjent sikkerhetsnivå, og løsningene lever i mange tilfeller sitt eget liv uavhengig av fylkeskommunens IT- og sikkerhetsavdelinger.

Hva må kommuner og fylkeskommuner gjøre?
Først og fremst må virksomheten igangsette gjennomganger av alle driftskontrollsystemer som de har ansvaret for. Medlemmene i Kommune-CSIRT får støtte av oss til disse prosessene, og vi har utviklet metoder for slik gjennomgang basert på erfaringsgrunnlaget fra mange kommunale løsninger kombinert med generell cybersikkerhetskompetanse.

Det er en klar fordel å ha en ekstern og 'nøytral' tredjepart som kan bidra med sin erfaring i dialogen mellom etat, kommuneledelse og IT-drift. En slik tredjepart kan også være et kommersielt selskap som har erfaring denne typen styringssystemer. Det er også fornuftig å ta med leverandørene i gjennomgangen – de sitter ofte på supplerende teknisk kunnskap om systemene, og står som oftest bak hele eller deler av løsningsdesignet.

Ved starten av 2023 er situasjonen at vi fortsatt har krig i Europa og en flora av organiserte cyberkriminelle og økt aktivitet av statssponsede trusselaktører med det vi kan kalle 'hevn-hacktivisme'. Eksempel på sistnevnte er tjenestenektangrep mot norske nettjenester utført av russiske hackere fordi Norge støtter Ukraina med våpen. Sett i lys av dette må kritisk infrastruktur i norske kommuner og fylkeskommuner være ekstra godt beskyttet. Her bør det settes inn ekstra innsats.

Situasjonsbilde – fjoråret sett i perspektiv

2021 var et «annus horribilis» for digital sikkerhet i Norge og sannsynligvis også internasjonalt. Vi kan nevne hendelser som Østre Toten, Drammen VA, Colonial Pipeline, Kaseya, hacking av Stortingets epostserver, Volue, Nordland fylkeskommune, Nortura og Amedia. Vi var forberedt på at 2022 kunne bli like ille, og et nytt faremoment ble introdusert gjennom krigsutbruddet i Ukraina 24. februar.

Slik ble det ikke i Norge, i hvert fall ikke når det gjelder kommuner og andre offentlige virksomheter. Det er observert en klar nedgang i antall vellykkede angrep og kompromitteringer, selv om noen private selskaper i Norge har blitt rammet av digital utpressing den siste tiden. En av de mest alvorlige hendelsene i 2022 er etter vår vurdering Norkart sin sårbarhet/feilkonfigurering som medførte tyveri av opplysninger om 3 millioner eiendomsbesittere i Norge. Nevnes bør også tjenestenektangrepene mot viktige nasjonale tjenester/funksjoner som Altinn, Stortinget og Nasjonal sikkerhetsmyndighet (NSM). Mot slutten av fjoråret ble Rec Silicon og Stangeland Maskin tatt av ransomware/digital utpressing. Likevel peker analysen totalt sett mot en viss nedgang i antall vellykkede cyberangrep, særlig når det gjelder de mest alvorlige angrepene.

I resten av Europa har cyberangrepene tilsynelatende ikke avtatt i styrke. Mot slutten av fjoråret ble det rapportert om vellykkede cyberangrep mot kommuner blant annet fra Sverige, Danmark Tyskland, Bulgaria, Nederland og Italia. Leverandører av sikkerhetsutstyr (brannmurer, VPN) melder om en kraftig økning av cyberangrep globalt – mellom 30 % og 80 % flere angrep fra 2021 til 2022, avhengig av land og sektor. En mulig forklaring på at vi har hatt færre vellykkede angrep, men flere angrep totalt, er at de fleste virksomhetene – i det minste i norsk offentlig sektor – var bedre sikret i 2022 enn i 2021. Ukraina-krigen og oppfordringen om økt årvåkenhet har sannsynligvis bidratt til bedre sikkerhet og dermed færre alvorlige hendelser. Vår vurdering samsvarer med NSM sine foreløpige observasjoner og analyser av cyberhendelser i 2022.

Mot slutten av fjoråret ble det observert en ny type angrepsmetodikk fra avanserte trusselaktører. De ser ut til å ha utviklet større grad av automatikk når det gjelder inntrenging og aksjoner på målet, og kan derfor nå flere og kompromittere raskere enn tidligere. Dette gjelder spesielt angrep mot sårbare, lokale MS Exchange-servere (e-posttjenere). Trusselaktører som antas å stå bak disse mer automatiserte angrepene er den forholdsvis nye aktøren *PLAY* og den mer velkjente *FIN7*. Konsekvensen av denne nye trusselen er at man i sterkere grad enn før må sørge for at lokale Exchange-servere er oppdatert til enhver tid.

Rundt årsskiftet ble det observert en bølge med nye cyberangrep – utover de som er nevnt over - mot både nordiske myndigheter og kommuner (det danske forsvaret, Dansk Nasjonalbank, to kommuner på Øland i Sverige), media (norske TV2) og næringsliv/industri (DNV). Og så blir det verre: I begynnelsen av

DIGITALT SITUASJONSBILDE

Kommune-CSIRT

2023 kommer en ny bølge med kompromitteringer av norske kommuner og virksomheter samt tjenesteangrep mot norske sykehus. Dette styrker vurderingen av at angrepsvolum og alvorlighet går i bølger, og at risikoen derfor fremdeles er høy for å bli angrepet og kompromittert.

Hovedvurdering
I lys av Ukraina-krigen, hevnangrep mot norske online-tjenester, sabotasje mot gassrørledninger, nye kompromitteringer av norske kommuner, forsvarets hevede beredskap og mistenkelige aktiviteter utført i landet vårt av personer fra nabolandet i øst, vurderer vi risikonivået uforandret fra i fjor høst og man bør fortsatt være årvåkne og sørge for best mulig sikring av kommunenes og fylkeskommunenes digitale systemer.

Kommune-CSIRT anser fortsatt digitalt angrep med dobbel utpressing fra avanserte, organiserte kriminelle som den mest alvorlige trusselen mot norske kommuner og fylkeskommuner. Samtidig kan kritisk infrastruktur som vannforsyning være spesielt sårbar og bør kontrolleres.

Glasskula – hva ser vi komme?

Etter å ha lagt 2022 bak oss, kan vi konkludere med at det store rushet med digitale angrep rundt jul uteble. Eller kanskje vi skal si at de var mislykkede, for antall angrep har ikke gått ned. Men hva skjer i begynnelsen av 2023? Jo, en rekke angrep og kompromitteringer av norske kommuner og virksomheter.

I vår analyse og utsikter for 2023 forventer vi fortsatt et høyt volum av digitale angrep. Både hevn-hacktivisme (jfr. tidligere nevnt hevnaksjoner mot nasjoner som støtter Ukraina), sofistikert phishing, forsyningskjedeangrep (angrep via underleverandører, programvareleverandører eller IT-partnere) og kompromittering via eksponerte tjenester vil forekomme, med dertil muligheter for eksempelvis digital utpressing/ransomwareoperasjoner. Det samme gjelder kombinasjonsangrep hvor svindlere benytter både epost og telefon for å overbevise ofrene om å utføre uheldige handlinger som medfører svindel eller kompromittering.

Nyere metoder som vi vil se mer av i 2023, er MFA-omgåelse og kanskje metaverse-angrep.

Førstnevnte gjelder multifaktorautentisering (MFA) som, til tross for å bidra til høyere sikkerhet, også kan omgås. Det kan gjøres ved å vise et falskt innloggingsbilde til f.eks. MS 365, som ofte kommer uventet, og dermed kan svindlerne høste inn innloggingsdetaljer. Disse benyttes videre inn til den reelle kontoen, og 2-faktor funksjonen trer i kraft som forventet og brukeren bekrefter. Man kan også bli offer for MFA-utmattelse, dvs. at det kommer så mange meldinger om MFA-autentisering at man til slutt gir etter. Dette kan typisk skje hvis brukernavn og passord er på avveie, men MFA gjør at dette ikke er nok til å komme inn på kontoen. Vi vil understreke at innføring av **MFA anbefales sterkt, og gir en MYE høyere sikkerhet enn singlefaktor-autentisering** (singelfaktor-autentisering eksempel: brukernavn + passord)!

Metavers (meta univers) tilbyr virkelighetsflukt gjennom bruk av VR-headset som gir brukeren tredimensjonal virtuell virkelighet hvor du kan treffe venner, handle og spille spill. Men man kan også kommunisere med kunder/brukere og drive informasjons- og forretningsvirksomhet. Store norske virksomheter og etater tester for tiden ut deltagelse og informasjonsvirksomhet i slike metavers. Et eksempel på et aktuelt metavers er Decentraland hvor blant annet Brønnøysundregistrene og Skatteetaten har etablert seg med informasjonsvirksomhet.

I slike metavers-tjenester ser man for seg mulige framtidige trusler som identitetstyveri, digital utpressing, pengevasking, digitale overgrep mot barn og falsk informasjon. Her må leverandørene sørge for strenge sikkerhetsmekanismer for å hindre ondsinnede aktører adgang til metaverset.

Figur 33: What is metaverse? (Ars Technica)

Når metavers nevnes som mulige angrepsmål for ondsinnede aktører, må vi nok se lenger enn 2023 før dette blir et reelt problem. Kanskje snakker vi om 5 år fram i tiden. Og metavers *kan* jo være en flopp eller boble. Men virtuelle virkelighetstjenester har kommet og gått i ulike utforminger i mange år, og noen tjenester vil overleve og bli banebrytende. Og når viktige etater og virksomheter som skatteetaten og banker er på plass i metavers, finnes også interessante, potensielle ofre for kriminelle der. Vi bør være oppmerksomme på at ondsinnede aktører også her vil prøve å utnytte nye digitale tjenester til sin fordel.

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:

Regjeringen.no – Meld. St. 9 (2022-2023) Nasjonal kontroll og digital motstandskraft for å ivareta nasjonal sikkerhet – Så åpent som mulig, så sikkert som nødvendig:
https://www.regjeringen.no/no/dokumenter/meld.-st.-9-20222023/id2950130/?ch=3

Nasjonal sikkerhetsmyndighet – Risiko 2023: Økt uforutsigbarhet krever høyere beredskap:
https://nsm.no/regelverk-og-hjelp/rapporter/risiko-2023

Etterretningstjenesten: Fokus 2023: Krigen i Ukraina er et tidsskille for Europa:
https://nsm.no/regelverk-og-hjelp/rapporter/risiko-2023

Politiets sikkerhetstjeneste – Nasjonal trusselvurdering 2023:
https://www.pst.no/alle-artikler/trusselvurderinger/ntv-2023/

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.**