DIGITALT SITUASJONSBILDE

Kommune-CSIRT

Rapport nr. 1 – 2021

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 fra medio desember til ultimo mars.

Sammendrag

Første kvartal 2021 har vært spesielt for norske kommuner. I januar skjedde det mest alvorlige cyberangrepet en norsk kommune har vært utsatt for noen gang. Den kriminelle aktiviteten i cyberdomenet har siden nyttår vært stor, og man har sett en stor pågang mot offentlig institusjoner i utlandet og i Norge, samt også private virksomheter i Norge. Det er utfordrende å følge med på utviklingen og samtidig sørge for et akseptabelt nivå på informasjonssikkerheten ut fra dagens trusselbilde.

I Situasjonsbilde for Q4 2020 skrev K-CSIRT «Vi håper denne typen angrep ikke rammer norske kommuner og fylkeskommuner, men vi frykter det verste». Dette gjaldt da løsepengevirusangrep med såkalt dobbel utpressing. Dessverre ble Østre Toten Kommune hardt rammet av et slikt angrep rett over nyttår. 10 januar leste vi på NRK.no *«Sensitiv pasientinformasjon kan være på avveie etter dataangrep. Datasystemet til Østre Toten kommune er angrepet og gjort utilgjengelig for alle ansatte. – Personnummer og helsedata kan være på avveie, sier ordføreren».* I etterkant av angrepet har løsepengevirusaktøren (PYSA) sin nettside på det mørke nettet vært utilgjengelig, noe som har gjort at vi ikke har sett data bli offentliggjort. 30. mars skjedde dessverre dette. Et lite utsnitt av dataene som var hentet ut under angrepet var nå lekket på det mørke nettet, og noe av informasjonen antas å inneholde sensitive personopplysninger.

Hovedsakelig er det to ting Q1 2021 vil bli husket for. Østre Toten kommune og sårbarheten i Microsoft Exchange servere. 2. mars ble det offentliggjort en nulldagssårbarhet på lokale Microsoft Exchange-servere. Nasjonal Sikkerhetsmyndighet var raskt ute og varslet om utnyttelse av sårbarheten. Sårbarheten var blitt utnyttet over lengre tid av en kinesisk hackergruppe som Microsoft kaller Hafnium. Hendelsen fikk konsekvenser også i Norge. Stortinget ble rammet, og etter det som er kjent, en kommune. Dog valgte mange kommuner å ta ned sine epost-systemer «for sikkerhets skyld». Det ble satt inn betydelige ressurser, både eksterne og interne, for å rydde opp i sårbarhetene, og for å sjekke om de var kompromittert. K-CSIRT støttet NSM i varsling og oppfølging av om lag 50 kommuner.

I begynnelsen av februar ble et vannverk i Florida hacket. Inntrengeren forsøkte å 100-doble tilsetningen av natriumhydroksid(natronlut) i vannet. Heldigvis ble endringen observert og umiddelbart tilbakeført av anleggsoperatøren. Kort tid etter dette ble et vannverk i en norsk kommune utsatt for et hackerangrep. Kommunen gikk raskt ut med informasjon om at situasjonen var under kontroll. Vann og avløp er et kommunalt område som har til dels store utfordringer innen digital sikkerhet. K-CSIRT har derfor et spesielt søkelys på sikkerheten for dette området.

Om vi vender blikket og ser fremover vil vi fortsatt advare mot phishing og svindelforsøk som benytter den pågående vaksineringsprosessen som tema og agn. Det har vært en rekke phishingangrep spesielt mot privatpersoner som tilsynelatende blir kontaktet om noe rundt tema - vaksinering. Andre tema vi også kan regne med at vil bli benyttet i phishingkampanjer fremover er Sharepoint/Teams som man stadig ser, og ikke minst Stortingsvalget når det nærmer seg.

K-CSIRT sin vurdering er at mange aktører fortsatt vil benytte løsepengevirus. Det er viktig å gjøre de tiltak man kan for å forhindre denne typen angrep, og samtidig gjøre virksomheten i stand til å kunne håndtere en slik hendelse hvis det fører til kompromittering.

Hendelser

Fra 18. desember og frem til uke 15 har vi sett et økende angrepsvolum mot offentlig og privat sektor, nye tilfeller av kompromitterte e-postkontoer, løsepengevirus og sikkerhetsbrudd. I denne delen av situasjonsbilde setter vi opp hendelser som har skjedd gjennom den siste perioden kronologisk. Listen er ikke uttømmende, og vi setter søkelys på hendelser som kan være relevant for kommunal og fylkeskommunal sektor. Ut over de hendelsene som nevnes har K-CSIRT varslet kommuner om en rekke kompromitterte kommunale e-postkontoer som er blitt benyttet i phishing. K-CSIRT følger opp varsler og håndterer slike hendelser umiddelbart.

Cyberangrep mot det finske parlamentet

Det finske parlamentet offentliggjorde 28.12 at de ble utsatt for et cyberangrep høsten 2020. Angrepet ble oppdaget av det tekniske overvåkingssystemet i parlamentet. Dette omhandlet kompromitteringer av e-postkontoer til blant andre parlamentsmedlemmer. Finsk politi hevdet at det i denne saken så ut til å være ukjente gjerningspersoner som gjennom cyberangrepet hadde kunnet fremskaffe opplysninger som enten var til fordel for en annen stat, eller med den hensikt å skade Finland. Politiet bekrefter at flere personer er rammet av angrepet.

EMOTET igjen aktiv

EMOTET startet opp igjen aktiviteten i midten av desember. Norske kommuner ble for det meste rammet rett før jul. Litauen ble også rammet av EMOTET i jula – et angrep som liknet mye på angrepet mot Hedmarkskommunene i september i fjor.

DDoS mot norske kommune

Distribuerte tjenestenektangrep (DDoS) fortsatte i første kvartal mot norske kommuner. 5.1.2021 ble et angrep gjennomført kl. 00.00 med en styrke på 14 Gbps mot en norsk kommune. Nettsiden til kommunen ble tatt ned i en kort periode. Det ble rapportert om flere DDoS- angrep mot flere kommuner gjennom store deler av januar. Angrepene pågikk ofte flere ganger pr. dag mot samme kommune. Ikke store mengder data, men nok til å ta ned kommunens nettsider.

Alvorlig ransomware angrep mot norsk kommune

9. januar, kl. 00.30 ble Østre Toten rammet av et alvorlig ransomwareangrep med utpressing. Den kriminelle aktøren – PYSA – krypterte alle serverne og slettet backup. Kommunen hadde ikke offline sikkerhetskopier, men tekniske undersøkelser avdekket flere VM-snapshot (komplett «bilde» av en virtuell server med minne og lagring) som ikke var kryptert, og som det var mulig å hente ut data fra. Angrepet satte kommunen kraftig tilbake, og det var tilbake til penn og papir ved mange av kommunens tjenesteområder. Kommunen fikk etter hvert støtte fra både kommersielle leverandører, KS og K-CSIRT. Kommune-CSIRT sendte ut varsel sammen med DSB og NSM samme helg som hendelsen skjedde til samtlige kommuner.

Teknologileverandøren AKVA Group rammet av et cyberangrep

Søndag 10. januar ble teknologileverandøren AKVA Group rammet av et cyberangrep og flere nøkkelsystemer i selskapet ble tatt ned. AKVA Group bekrefter til Dagens Næringsliv at det var snakk om et løsepengevirus. Angriperne fikk i dette tilfellet tak i, og krypterte, produksjonsdata fra et ERP-system.

DDoS angrep mot mediehus

Tirsdag 12. januar kunne Hamar Media meddele at de var utsatt for et DDoS angrep. Allerede lørdag 9. januar merket de uregelmessigheter i trafikken. Hamar Media fikk store problemer med både å produsere og legge ut nyheter. Dette rammet trafikken og nettet for hele Hamar Media som totalt bidro til utfordringer for fire aviser i nærområdet.

Alvorlig dataangrep i Frankrike

21. januar: Vienne, et fransk departement med 38 kantoner og 218 kommuner ble rammet av et dataangrep. Alle datamaskiner tilknyttet departementet kom ut av drift, og telefonnettverket ble sterkt forstyrret. Viruset som i en periode hadde vært aktivt i Frankrike hadde infisert datasystemene til lokalsamfunn, departement, og også private selskaper. Noen uker tidligere ble bydelen La Rochelle berørt av et angrep av samme type, enkelte kilder melder om at aktøren var NetWalker. Hackerne krevde løsepenger. Omfanget av skaden og kostnadene ved dette angrepet er ikke kjent.

EMOTET botnet ble tatt ned

26. januar: EMOTET botnet ble tatt ned gjennom en samordnet aksjon med Europol. Myndigheter fra åtte land bidro til å ta ned infrastrukturen til Emotet. Dette er en beryktet e-postbasert Windows-malware som står bak flere botnet-drevne spamkampanjer og ransomware-angrep det siste tiåret. Den koordinerte fjerningen av botnet 26. januar - kalt "Operasjon Ladybird" – var resultatet av en felles innsats av myndigheter i Nederland, Tyskland, USA, Storbritannia, Frankrike, Litauen, Canada og Ukraina.

Vannverk i Florida hacket

5. februar ble et vannverk i Florida hacket. Angrepet på Oldsmar vannverk skjedde gjennom en remote desktop programvare som gjorde uautoriserte brukere i stand til å gjøre omkonfigurering av systemene fra utsiden. Inntrengeren tilbrakte mellom tre til fem minutter inne i systemet og forsøkte å 100-doble tilsetningen av natriumhydroksyd(natronlut/lut). Endringen ble umiddelbart tilbakeført av anleggsoperatøren, og befolkningen i Oldsmar var ikke i fare på noe tidspunkt. *Kommune-CSIRT sendte på bakgrunn av hendelsen et varsel til alle norske kommuner. Varselet ble utarbeidet av KraftCERT i samarbeid med Kommune-CSIRT og Norsk Vann.*

Norsk kommune utsatt for dataangrep mot infrastruktur for vann og avløp

16. februar ble en norsk kommune utsatt for et hackerangrep mot «en mindre del av infrastrukturen for vann og avløp». Kommunen uttrykte raskt at de hadde kontroll på situasjonen, og at alle vann- og avløpssystemer fungerte som normalt. Ingen av kommunens innbyggere ble berørt av situasjonen, og ingen personopplysninger antas å være på avveie.

Løsepengevirus angrep mot TietoEVRY

22. februar fikk TietoEVRY tekniske problemer med flere tjenester de leverer. 25 kunder som hovedsakelig er innen handel, industri og tjenesteytende næringer, ble berørt. Undersøkelser viste at hendelsen skyldtes et løsepengevirusangrep (ransomware). TietoEVRY anså hendelsen som en alvorlig kriminell handling. Den berørte infrastrukturen og tilknyttede tjenester ble, som et forebyggende tiltak, skrudd av. Systemer og relevante data måtte reetableres på en kontrollert måte.

Utsendelse av phishing-e-post fra en norsk kommune

25. februar meldte en norsk kommune at de var utsatt for et dataangrep. Det ble sendte ut en stor mengde phishing-e-post fra en e-postkonto tilhørende kommunen. Tematikken i e-posten omhandlet COVID-19 og oppdatering av et meldingssystem. De kriminelle spiller på frykt, og det kommer frem av e-posten at «*Hvis du ikke kan fylle ut informasjonen, blir kontoen din deaktivert».* Emnefeltet på e-posten viser gjerne til Systemadministrator eller IT Service Help Desk.

Nulldagssårbarhet i MS Exchange Server

2. mars melder Volexity og etter hvert også Microsoft (MS), om en nulldagssårbarhet i MS Exchange Server som er meget alvorlig og kritisk for alle som har egne Exchange e-postservere. Den hadde blitt utnyttet av kinesiske hackere i lang tid, og da dette ble offentliggjort, publiserte Microsoft en hasteoppdatering (såkalt out-of-band oppdatering). Publiseringen medførte et rush av angrep over hele verden for å utnytte sårbarheten til kriminelle handlinger. K-CSIRT varslet medlemmene sine samt et 50-talls kommuner som hadde sårbare servere stående, og de fleste ble sikret. Hele uken fra 2. mars til 5. mars ble preget av travel varsling og utveksling av opplysninger rundt denne alvorlige sårbarheten.

Norsk kommune rammet av sårbarhet i Microsoft Exchange

9. mars offentliggjorde en norsk kommune at de var rammet av et IT-angrep gjennom sikkerhetshull i Microsoft Exchange. Dette er samme sårbarhet som nevnt over. Kommunen bestemte samme dag å ta ned deler av de kommunale systemene for å håndtere situasjonen. Kommunen uttalte at det ikke fantes indikasjoner på at sensitiv informasjon var på avveier, og det ble iverksatt ekstra tiltak for å sikre systemer og data.

Stortinget rammet av dataangrep

10. mars ble det kjent at Stortinget var blitt rammet av et dataangrep. Stortinget ble varslet om angrepet fra Nasjonal sikkerhetsmyndighet som meldte fra om unormal aktivitet inn mot Stortinget. Innbruddet skjedde ved hjelp av en sårbarhet i Microsofts Exchange. Sårbarheten er den samme som nevnt i de to foregående hendelsene. Stortingspresidenten omtalte datainnbruddet «som et angrep på vårt demokrati». Mange ble rammet, og dette angrepet fremsto som større og mer avansert enn angrep Stortinget ble utsatt for i august 2020.

Et av Londons største akademier rammet av løsepengeangrep

27. Mars ble et av Londons største akademier, Harris Federation, rammet av løsepengeangrep. De ble tatt av den avanserte aktøren REVil/Sodinokibi. IT-systemer, e-postservere og telefonlinjer ved primær- og sekundærakademier gikk ned over hele London. Hendelsen representerer det største ransomware-angrepet som hittil er kjent mot en utdanningsinstitusjon i Storbritannia. Harris Federation består av 48 skoler og utdanner rundt 36 000 barn hvert år. Skolemyndighetene skrev i en pressemelding at hendelsen ble etterforsket sammen med et sikkerhetsfirma, UK National Crime Agency og UK NCSC.

Situasjonsbilde og vurderinger:

Ransomware/løsepengevirus med dobbel utpressing – en sterkt økende trend

I forrige Situasjonsbilde publisert 18. desember i fjor, advarte vi mot denne trusselen og fryktet at norske kommuner ville bli angrepet. Kun få dager inn i det nye året – lørdag 9. januar - ble K-CSIRT kontaktet av Østre Toten kommune. De var blitt offer for et vellykket ransomwareangrep av en avansert aktør som kaller seg PYSA. Hele den virtuelle serverparken til kommunen ble kryptert og låst ned – inkludert deres online backup-løsning hvor også sikkerhetskopiene ble slettet. Aktøren hadde også stjålet betydelige mengder data, og dobbel utpressing fremstod som et mulig scenario. Kommunens operative evne ble sterkt redusert – pressen fortalte om manuelle bjeller på sykehjem, og skoler og administrasjon som måtte tilbake til penn og papir.

Situasjonen ble ytterligere forverret den 29. mars. Da offentliggjorde PYSA på det mørke nettet det man vurderer som deler av de data de hadde stjålet fra kommunen. Dobbel utpressing-scenarioet var et faktum. Dermed fikk kommunen nok et problem å hanskes med. De måtte håndtere sensitive personopplysninger på avveie, og informere og støtte personer som ble rammet. Totalt sett en svært vanskelig situasjon for en kommune som allerede var i krise på grunn av nedlåsingen av eksisterende systemer og data.

Gjennom nyhetsbildet og andre kilder ser vi at aktørene blir flere, nedslagsfeltet bredere (type ofre) og arbeidsdelingen mer omfattende blant de kriminelle. Tidligere gikk de avanserte aktørene for det meste etter de store, private bedriftene med høy omsetning, såkalt Big Game Hunting. Nå ser vi at mange offentlige virksomheter – fra universiteter til kommuner – i større grad blir angrepet av de samme kriminelle aktørene. De kriminelle har også en arbeidsdeling – man kan skaffe seg tilgang til en bedrift (hacke seg inn) for deretter å leie ransomware og tilhørende metode/prosess av en avansert aktør. Utleier av skadevare krever så en andel av «byttet» som betaling.

En annen type samarbeid er deling av infrastruktur, programvareutvikling og lekkasjesider på det mørke nettet. Et slikt samarbeid antas å finne sted mellom aktører som går under navnene Maze, Egregor, Lockbit, SunCrypt og RagnarLocker med flere. Sikkerhetsselskapet Analyst1 publiserte en rapport i begynnelsen av april hvor de viser til blant annet delte lekkasjesider, delt infrastruktur og andre måter de samarbeider på. Analyst1 kaller dette et mafia-kartell.

Innsatsfaktorene til de kriminelle er små, de trenger kun en datamaskin, internettilgang og hackingkompetanse. Gevinstene kan derimot være enorme, utpressingsbeløpene går fra 1 million kroner og oppover, og er økende. Når det i tillegg viser seg at mange velger å betale, bidrar dette til flere angrep og høyere beløpskrav. Sikkerhetsselskapet Kaspersky melder i en nylig utgitt rapport at 56 % av 15.000 rammede virksomheter betalte løsepenger. Østre Toten meddelte fra dag én at de ikke kom til å betale utpresserne. Det er en beslutning det står respekt av, og vi håper flere følger Østre Toten.

Vår vurdering er at lønnsomheten kombinert med arbeidsdelingen blant de kriminelle gjør at risikoen for denne typen angrep vil øke fremover. De kriminelle er svært raske til å utnytte nye sårbarheter som blir oppdaget, og derfor vil gode sikkerhetsprosedyrer og rask handling være avgjørende for å unngå å bli tatt.

Kommune-CSIRT anbefaler følgende tiltak mot denne typen angrep:
Preventive:

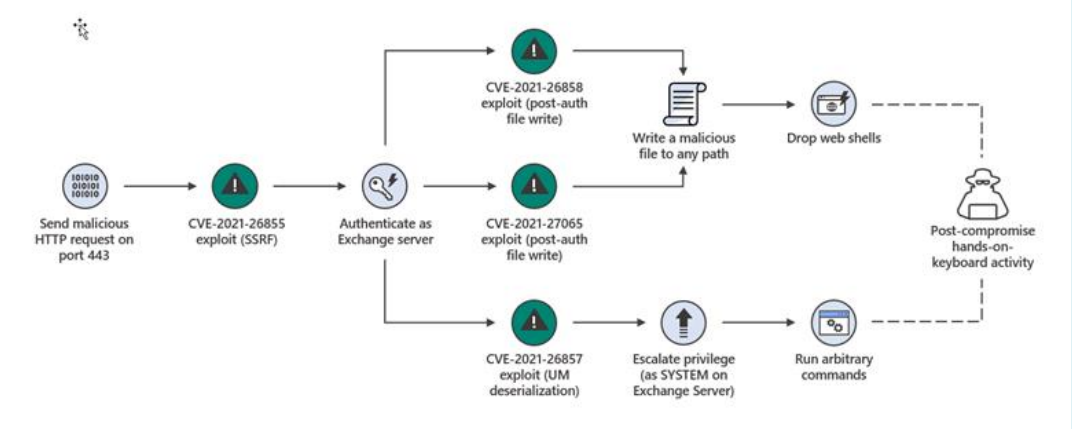
- Installer sikkerhetsoppdateringer så snart de er publisert - for alle typer programvare
- Reduser antall eksternt eksponerte tjenester til et minimum, og fjern utrangerte systemer
- Bruk multifaktor-autentisering der det er mulig. Spesielt viktig for eksternt eksponerte tjenester, og gjør ingen unntak når en tjeneste får denne mekanismen!
- Unngå gjenbruk av passord på tvers av kontoer
- Overvåk brukerkontoer med administrator-rettigheter og gi tilganger med lavest mulige rettigheter.
- Bruk mekanismer for å redusere en vanlig brukers muligheter til å kjøre ukjent kode (ATP, DEP, etc)
- Kontinuerlig trening av ansatte og brukere i sikkerhetsbevissthet (phishing, passord etc)
- Hvis mulig: Bruk sandkasser for vask av epost og sperr for klikking på lenker

Skadereduserende tiltak (reduserer effektene av kompromittering):

- Sørg for å ha sikkerhetskopier oppbevart reelt offline.
- Bruk nettverkssegmentering for å hindre intern spredning
- Utarbeid og operasjonaliser prosedyrer for hendelseshåndtering og gjenoppretting

Utnyttelse av kritiske sårbarheter

Som nevnt under hendelser ble det 2. mars offentliggjort en nulldagssårbarhet på lokale Microsoft Exchange-servere. Svakheten var blitt utnyttet over lengre tid av en kinesisk hackergruppe som Microsoft kaller Hafnium. Denne sårbarheten kombinert med andre, kjente sårbarheter, kunne benyttes til å skaffe aktører forhøyede rettigheter og mulighet for å installere webshell (et web-shell er en bakdør på en web-server). Da metoden for å utnytte sårbarheten ble offentlig, startet et rush over hele verden med angrep mot sårbare installasjoner. I Norge så man et enormt trykk fra og med morgenen onsdag 3. mars. Mange tusen norske servere var sårbare og mange ble angrepet. Hele sikkerhetsmiljøet med sektorCERTene i spissen jobbet intenst hele uken med varsling og oppfordret til oppdatering. Dette gjaldt også Kommune-CSIRT som varslet og fulgte opp et 50-talls norske kommuner som var sårbare. Kommune-Norge er i skrivende stund oppdatert og noenlunde trygge mot akkurat denne trusselen, med mindre de var kompromittert allerede før oppgraderingen.



Figur 1: Angrepsflyten ved utnyttelse av Exchange-sårbarhetene (Ill: Microsoft)

Sårbarheten hadde betydelige konsekvenser i Norge. Stortinget ble som kjent rammet, det samme gjelder en norsk kommune og et transportselskap i Trøndelag. Flere kommuner og driftsselskaper tok ned epost-systemet «for sikkerhets skyld». Mange kommuner satte inn betydelige ressurser, både eksterne og interne, for å rydde opp i sårbarhetene og for å sjekke om de var kompromittert. Mange var heller ikke klar over at sårbarheten kunne ha resultert i komplett kompromittering, kryptering og utpressing ala Østre Toten hvis de rette aktørene hadde kommet til.

Aktivitetene til både angripere og forsvarere ved denne sårbarheten, understreker noe vi har meddelt i flere sammenhenger – nemlig at utnyttelsen av sårbarheter både går raskere og skjer i større volum enn tidligere. Det krever et årvåkent sikkerhetsmiljø med handlekraft, og at norske kommuner, fylkeskommuner og andre både har varslingskanaler og er i stand til å reagere raskt.

Glasskula – hva ser vi komme?

Angrepene mot norske kommuner vil fortsette som før og antagelig øke noe de neste månedene. Vi er i en situasjon hvor det skjer mange samtidige endringer hos kommuner og fylkeskommuner. De er i flere transformasjonsfaser, både mot mer digitalisering og mer skytjenester. Dette gir mer sårbare systemer og økte muligheter for ondsinnede trusselaktører.

Mest alvorlige trussel fremover: Avansert løsepengeangrep med dobbel utpressing.
Samtidig som enkelte aktører blir tatt gjennom effektivt internasjonalt politisamarbeid (EMOTET, Egregor mfl.), har vi den siste tiden også observert stadig nye aktører, skadevare og prosedyrer blant de kriminelle.

En slik ny aktør, av noen kalt Cring, går aktivt etter spesielle nettverksprodukter som Fortinet SSL-VPN med sårbart FortiOS operativsystem. Den alvorligste sårbarheten gir full dump av alle brukernavn og passord på enheten. Cring angriper gjerne tekniske installasjoner og industri.

En annen ny fare er en aktør kalt TA551. De har begynt å bruke IcedID-skadevaren – kjent som en banktrojaner – til å hacke seg inn hos virksomheter for å så å benytte seg av kryptering og dobbel utpressing. Det nye her er at de har en svært effektiv operasjon, den såkalte «time-to-ransom» (fra innbrudd til fullført kryptering) går på 1½ dag. De er mye raskere enn vanlig, noe som betyr at de er vanskeligere å oppdage i denne fasen.

Andre trusler
Vår vurdering er at phishing opprettholdes som en vesentlig trussel. Phishing-tematikk fremover vil inneholde aktuelle temaer som COVID-19/Korona, vaksiner og stortingsvalget 2021, i tillegg til de vanlige forsøkene med eksempelvis Posten som tema. Økt netthandel under pandemien fører også til økt simulering av kjente merkevarer og online-butikker som tilsynelatende ønsker å gi forbruker en gave. Phishing-kampanjer utføres nå både med epost, SMS ('smishing') og med telefonoppringning ('vishing' – v for voice).

I forbindelse med stortingsvalget til høsten, er det etter vår vurdering en økt fare for falske nyheter, falske arrangementer og falske identiteter på sosiale media. *Vår anbefaling er å være kritisk til informasjon og kontoer man finner i sosiale media som man ikke kjenner den reelle identiteten eller kilden til.*

Siste side

Rapportens aktuelle situasjonstips:

For brukere:

- Ikke aktiver innhold i vedlegg – ikke klikk på lenker verken i epost eller SMS
- Gjenbruk av brukernavn og passord er ingen god idé og bør unngås!

For driftspersonell:

- Ikke la utrangerte servere bli stående eksponert mot internett
- Hjemmekontor, digital undervisning og møter – hvordan kan sikkerheten der bli bedre?
- Oppgrader nettverkskomponenter som VPN og brannmur så raskt det lar seg gjøre - angrepene mot disse øker
- Gjennomfør andre tiltak som hindrer løsepengeangrep (se rapport, varsel fra NSM, DSB og K-CSIRT - https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/varsler-fra-ncsc/varsel-om-losepengevirus eller ta kontakt med oss)
- Sørg for å ha sikkerhetskopier som er reelt offline

Relevante Rapporter og dokumenter publisert i perioden:

02. februar - KS gir råd til kommuner for å redusere risiko for nye dataangrep. KS-brev til Kommunedirektør og IT-ansvarlig/IT-Sikkerhetsansvarlig
https://www.ks.no/fagomrader/digitalisering/styring-og-organisering/ks-gir-rad-til-kommuner-for-a-redusere-risiko-for-nye-dataangrep/

8. februar laserte de hemmelige tjenestene i Norge sitt trussel- og risikobilde.

NSM: Risiko 2021 – helhetlig sikring mot sammensatte trusler
https://nsm.no/getfile.php/136419-1616673370/Demo/Dokumenter/Rapporter/NSM_Risiko_2021_web_enkeltside_1203.pdf

Etterretningstjenesten: Fokus 2021 – Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer
https://www.forsvaret.no/aktuelt-og-presse/publikasjoner/fokus/rapporter/Fokus2021-web.pdf/_/attachment/inline/b9d52b53-0abe-4d1c-9c51-bf95796560bf:8dd66029b7efb38aab37d13e8b387d2e6ed0bd05/Fokus2021-web.pdf

PST: Nasjonal trusselvurdering 2021
https://www.pst.no/globalassets/artikler/trusselvurderinger/nasjonal-trusselvurdering-2021/ntv_2021_final_web_1802-1.pdf

24. mars – NorSIS: Trusler og trender 2021
https://norsis.no/wp-content/uploads/2021/03/NorSIS_Trusler_Trender_2021_Digital.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 4**