DIGITALT SITUASJONSBILDE

Kommune-CSIRT

Rapport nr. 2 – 2020

Rapporten er Kommune-CSIRT sin beskrivelse og vurdering/analyse av digitale trusler, sårbarheter og hendelser i kommunal og fylkeskommunal sektor. Perioden for analysen er fra ultimo september til medio desember.

Sammendrag

Fjerde kvartal fortsatte der tredje kvartal slapp, med økende angrepsvolum mot offentlig og privat sektor, nye tilfeller av kompromitterte e-postkontoer, løsepengevirus og sikkerhetsbrudd. Samtidig digitaliseres norske kommuner i et stadig høyere tempo. Det skal virkelig noe til å holde oversikt og følge med på utviklingen og samtidig sørge for et akseptabelt nivå på informasjonssikkerheten. Derfor påpeker vi igjen: *Det er et lederansvar (kommunedirektører og ordførere/politikere) å sørge for at digitalisering og sikkerhetsarbeid går i takt!*

Antall angrep fra løsepengevirusaktører øker i volum og antall aktører som står bak. Det multi-nasjonale selskapet Sopra Steria - som blant annet drifter tjenester for det offentlige Norge inkludert kommuner – ble utsatt for et avansert angrep og påfølgende kompromittering av intern infrastruktur i oktober. Vi håper denne typen angrep ikke rammer norske kommuner og fylkeskommuner, men vi frykter det verste.

VPN-løsning som tilkoblingsmetode til arbeidsplassen når du er på reise, hjemmekontor el. brukes stadig mer – særlig i disse hjemmekontortider. Samme type sårbarhet som ble omtalt i media i høst har blitt utnyttet på Fortinet sin VPN-løsning. Oppdatering/rettelse av denne svakheten har vært tilgjengelig siden 2019. I november kom Kommune-CSIRT over en liste med mer enn 49.000 sårbare VPN-løsninger av denne typen, hvorav 255 av disse var norske. Vi kan ikke få sagt ofte og tydelig nok: *Sørg for at kritiske løsninger blir oppdatert!*

Databaser med brukernavn og passord fra hackede tjenester på internett dukker stadig opp. Sist i november kom en ny samling av databaser som var enda større enn tidligere, og med en del nye oppføringer. Vi har informert - og arbeider fortsatt med å få ut informasjon til kommuner og fylkeskommuner som hadde treff her.

Flere alvorlige sårbarheter i nettverkslaget for små nettverksenheter - også kalt Internet of Things (IoT) - ble publisert i begynnelsen av desember, og aktualiserte dessverre vår antagelse fra forrige rapport om sårbarheten for IoT. En del leverandører vet heller ikke at de er berørt av denne feilen. Vår bekymring er at driftskontrollsystemer hos kommunene kan være berørt, det samme med enheter i velferdsteknologi og smarthus.

Kommune-CSIRT har avdekket at sensitiv informasjon fra kommuner og annen offentlig forvaltning har ligget åpent på anbudsportaler. Det legges ut detaljert, intern dokumentasjon om kritisk infrastruktur. Slik informasjon vil være gull verdt for terrorister, kriminelle og andre ondsinnede aktører. De som gjennomfører anbud, MÅ sørge for å unngå slike publiseringer.

Fremover vil vi spesielt advare mot phishing og svindelforsøk som benytter den kommende vaksineringsprosessen som tema og agn. Det er allerede observert infiserte skjemavedlegg i e-poster mot privatpersoner som tilsynelatende blir kontaktet for vaksinering.

En annen trend som kan bli mer utfordrende er digitalt utstyr, programvare og tjenester som benyttes i jobbsammenheng uten å være autorisert av IT-avdelingen – såkalt skygge-IT. Økende bruk av hjemmekontor og jobbing utenfor kontoret – kanskje nå også som en mer varig trend – aktualiserer problemene med skygge-IT for norske kommuner og fylkeskommuner.

Hendelser

Tjenestenektangrep på norske kommuner
Det har blitt observert tjenestenektangrep mot flere norske kommuner i hele perioden. Størrelsen på angrepene har vært i kategorien små til middels store, og vi har observert sammenfall med både kommunestyremøter og eksamen – uten at det dermed må være en sammenheng.

Norsk kommune med åpen tilgang til teknisk anlegg
I slutten av september avdekket Kommune-CSIRT at et teknisk anlegg eid av en kommune var eksponert på internett og kun beskyttet med standard leverandørpassord. Slike passord ligger fritt tilgjengelig på internett. K-CSIRT varslet den aktuelle kommunen om forholdet.

Flere epost-kontoer hos norske kommuner er blitt kompromittert
Vi har også dette kvartalet mottatt en rekke varsler om kompromitterte epost-kontoer hos kommuner. Dette er typisk kontoer som har blitt kompromittert gjennom phishing, og som brukes videre til å sende ut nye phishing-eposter og skadevare til andre mottagere. Vi har varslet en rekke kommuner i hele perioden fra september til desember.

Økende phishing med Posten pakkesporing
I slutten av november og begynnelsen av desember ble det observert en økning i phishing-aktivitet med Posten som tema. Her er det både forsøk på stjeling av kredittkortinformasjon og innhøsting av påloggingsinformasjon. Dette er ikke overraskende når vi tenker sammenfallende hendelser som jul, pandemi og netthandel. Denne typen svindel endrer gjerne innhold fra midten av desember til å omhandle uavhentede pakker på posten i stedet for pakker på vei. Metoden og målet er det samme.

Kommunalt bibliotek kompromittert
I slutten av september ble et kommunalt bibliotek utsatt for uautorisert tilgang til deres systemer gjennom et sikkerhetshull i et webhotell. Løsningen kommunen benyttet var et system som var utviklet i fellesskap og benyttes av mange kommuner. Sikkerhetshullet ble tettet og tilgangen herdet. Det er uklart om tilgangen har medført uthenting av personopplysninger, påloggingsinformasjon eller lignende.

Sopra Steria angrepet av Ryuk løsepengevirus
Den franske IT-giganten Sopra Steria som leverer tjenester til mange offentlige virksomheter i Norge – deriblant flere kommuner - ble 20. oktober infisert av Ryuk løsepengevirus. Bak denne skadevaren skjuler det seg en avansert kriminell aktør – av noen kalt WIZARD SPIDER – som går mot store private foretak med høy omsetning. Denne type operasjoner kalles ofte Big Game Hunting, fordi det kan være store penger å hente, og fordi angrepet er målrettet og krevende under planlegging og gjennomføring. Ifølge Sopra Steria ble ingen kundedata eller norske kunder skadet eller berørt.

I perioden har det også vært en rekke andre hendelser som har omhandlet løsepengevirus:

- Synsam – nordisk optikerkjede ble rammet av skadevaren/løsepengeviruset REvil/Sodinokibi i september
- CMA CGM – fransk transportfirma ble rammet av Ragnar Locker løsepengevirus sent i september.
- Enel Group – et italiensk energiselskap med kunder i 40 land - rammet av NetWalker løsepengevirus medio oktober – krevet for 14 Mill USD,
- Vastaamo Psykiatrisenter i Finland ble utsatt for løsepengevirus for to år tilbake. Virksomheten nektet å betale løsepenger. 40.000 psykiatriske journaler viste seg å være tatt ut av senterets IT- systemer, og har den senere tid blitt benyttet til utpressing av pasientene.
- Hurtigruten ble 14. desember rammet av løsepengevirus. Mange systemer ble satt ut av drift, blant annet selskapets hjemmesider.

Alvorlig sårbarhet i Fortinet sin VPN-løsning
En sårbarhet i VPN-løsningen til nettverksutstyrsleverandøren Fortinet – med produktnavn Fortigate - har medført at rundt 255 norske virksomheter har fått lekket brukernavn og passord til sin VPN-løsning. Sårbarheten (CVE 2018-13379) har vært offentlig kjent siden mai 2019, og oppdatering har også vært tilgjengelig og kommunisert fra samme tidspunkt. Igjen er det mangel på oppdatering som resulterer i lekkasjer og kompromittering.

I november 2020 ble det publisert en rekke lister med til sammen over 49.000 ip-adresser på utstyr som fortsatt hadde sårbarheten, noen dager senere kom det også lister med informasjon om brukernavn og passord. Sårbarheten berører samtlige sektorer og i Norge er det alt fra kommuner og andre offentlige virksomheter til forskning, utvikling av medisinsk utstyr, energi, transportfirmaer og fagforeninger m.fl. Kommune-CSIRT varslet en større nettverksleverandør som har kommunale kunder, og vi er også kjent med at minst to kommuner har vært berørt. Disse er varslet.

Passorddatabase-lekkasje
I slutten av november ble det publisert 26318 hackede databaser med påloggingsinformasjon på diverse hackerfora – inneholdende over 220 millioner unike kontoer. Rundt 50 % av disse er å regne som nye og til nå ukjente lekkasjer der brukeren ikke er kjent med at uvedkommende har tilgang til epostadresse og passord på tjenesten den er benyttet og andre steder hvor samme påloggingsdetaljer er anvendt.

16. oktober meldte E24 at 22.000 Schibsted-kontoer hadde blitt hacket ved hjelp informasjon fra slike databaser. Schibsted er et mediehus som eier blant VG, Aftenposten og Finn.no. Disse kontoene benyttes til betaling av både elektroniske og tradisjonelle tjenester, eksempelvis for merkenavnene over. Dette viser tydelig hvordan kriminelle benytter slike lekkasjer til å skaffe seg tilgang til nye tjenester og kontoer.

Norske bedrifter utsatt for distribuert tjenestenektangrep og krav om betaling.
Mandag 12. oktober ble Telenor Norge rammet av et betydelig tjenestenektangrep med krav om løsepenger. Angrepet mot den norske telegiganten varte i cirka tre timer, og de kriminelle forlangte 20 Bitcoin (ca. 2 millioner kroner) i betaling for å ikke følge opp med nye og kraftigere angrep. I en kort periode tok Telenor ned all trafikk inn til de berørte tjenestene. Tjenester som var utilgjengelig i omtrent en time var blant annet Telenors egne nettsider og e-post.

I november og desember ble vinmonopolet.no tatt ned av flere distribuerte tjenestenektangrep. Angrepenes trafikkmengde er registrert til henholdsvis 65 og 130 Gigabit per sekund mot selskapets infrastruktur. Angrepet i desember fikk store konsekvenser. All omsetning fra nettsidene stoppet opp, det ble umulig å gjennomføre kjøp med gavekort i butikkene og selskapets apper ble ubrukelige.

Manglende kontroll på elevers personvern
En fylkeskommune har varslet Datatilsynet om et brudd på personopplysningssikkerheten etter at strømmevideoer for 12 500 elever lå tilgjengelig for andre elever og ansatte i fylkeskommunen. Videoene viser både samtaler mellom elever, tilbakemelding fra lærere til elever, samt møter og kurs. Opptakene er gjort i Teams, og lagt ut i videodelingstjenesten Microsoft Stream. Personopplysningsbruddet ble oppdaget 9. juni, men fylket varslet først de berørte 16 oktober. Fylkeskommunen har rettet avviket.

Datatilsynet har på bakgrunn av bekymring hos flere foresatte sett nærmere på tre kommuner som har tatt i bruk Google Chromebook og G Suite for Education. Det ble avdekket betydelige mangler, og det ble offentliggjort et varsel om irettesettelse 11.12.20 på Datatilsynets hjemmesider.

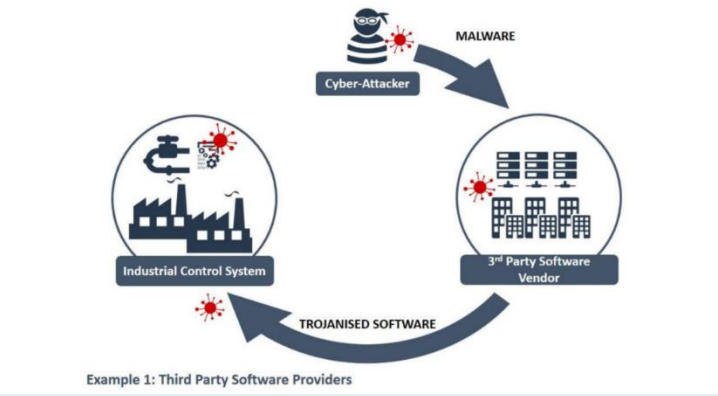
Covid-19-pandemien utnyttes av cyberkriminelle
Pandemien og dens brutale konsekvenser stopper ikke kriminelle fra å utnytte denne situasjonen – heller tvert om. Det er blitt observert – også i dette kvartalet – fakturasvindel i forbindelse med smittevernutstyr, phishing med COVID-19-tematikk og direkte hackingangrep på vaksineprodusenter. Sistnevnte produsenter er både kritiske for folkehelsen og har sannsynligvis bra med kapital, derfor anser de kriminelle at dette er attraktive mål.

Tekniske dokumenter om kommuners infrastruktur lå åpent på internett
Kommune-CSIRT har ved flere tilfeller kommet over dokumenter og skisser som i forbindelse med offentlige anbudskonkurranser er lagt ut på anbudsportaler. Det har eksempelvis vært komplett dokumentasjon på IKT-infrastrukturer som kan anvendes av en ondsinnet aktør som et veikart inn i virksomhetens elektroniske infrastruktur.

Kritisk sårbarhet avdekket i enkle, internett-tilkoblede enheter, såkalt Internet-of-Things enheter (IoT)
Hele 33 alvorlige sårbarheter i nettverkslaget for IoT. Sårbarhetene som går under fellesnavnet Amnesia:33 og ble publisert i begynnelsen av desember. Dette aktualiserte dessverre vår antagelse fra forrige rapport om hvor sårbare IoT-enheter er. Det er nettverks-bibliotekene i programvaren som er avslørt som meget sårbar - de 33 sårbarhetene er avdekket i de fire åpen kildekode-bibliotekene uIP, FNET, picoTCP og Nut/Net. Sårbarhetene eksisterer på et så lavt nivå at programvaren i mange tilfeller ikke lar seg oppgradere/patche. Programvare bibliotekene brukes i forskjellige enheter, fra driftskontrollsystemer for elforsyning fra Siemens til Teslas Car Area Network (CAN). Kontrollsystemer, enheter i velferdsteknologi og eventuelle smarthus hos kommuner kan være berørt.

Programvareleverandøren Solarwinds rammet av forsyningskjedeangrep
Hos den amerikanske leverandøren av system- og nettverksstyring, Solarwinds, ble det i begynnelsen av desember avslørt infiserte versjoner av deres programvare Orion. Disse infiserte versjonene har blitt brukt til å oppgradere kundenes systemer i løpet av de siste ni månedene. Kundenes systemer kan derfor være infiserte, og aktøren bak angrepet kan da åpne en bakdør hos kunden som gjør at aktøren kan utføre handlinger på rammet infrastruktur (for eksempel spionasje, sabotasje og spredning).

Solarwinds har både kritiske og høyt profilerte kunder som US Air Force, US Secret Service, US Dept of Defense, DHS, Microsoft, Telenor, Equinor, Volvo, Cisco og FireEye (et av de største cybersikkerhets-selskapene i verden). Totalt har selskapet mer enn 300.000 kunder, og det meldes at ca. 18.000 av disse har lastet ned den infiserte skadevaren. Det er likevel ikke kjent hvilke selskaper som er rammet – det foreligger ingen åpen oversikt over *hvem* som har lastet ned de skadelige versjonene. Sett i lys av hvem de mulige ofrene er og at angrepet er svært avansert, spekuleres det i åpne kilder i at aktøren er statssponset og antagelig har tilknytning til russisk etterretning.



Illustrasjon: Forsyningskjedeangrep – Supply Chain Attack (Kilde: NCSC-UK)

Situasjonsbilde og vurderinger:

Et økende digitaliseringspress, mer sofistikerte cyberangrep, ulike typer lekkasjer og publisering, og nye arbeidsformer gir utfordringer for norske kommuner og fylkeskommuner. I denne vurderingen vil vi se litt på hva dette kan innebære av konkrete trusler og sårbarheter.

Løsepengevirus er den største trusselen

De omtalte hendelsene som inneholder løsepengevirus er eksempler på alvorlig cyberkriminalitet med kryptering av selskapets dokumenter, påfølgende pengeutpressing, og trussel om offentliggjøring av sensitive data. Så langt har vi ikke informasjon om at denne typen angrep har rammet norske kommuner og fylkeskommuner, men vi må være forberedt på at det kan skje.

Under et angrepet mot en rekke kommuner i Innlandet i september hadde en kriminell aktør mulighet for å spre løsepengevirus, men gjorde det ikke. Ofte selger den som klarer å infisere et system, denne tilgangen til andre kriminelle. Kjøperne benytter deretter det infiserte systemet til sitt formål, og det er denne aktøren som avgjør hvordan det kompromitterte systemet skal utnyttes.

Ifølge åpne kilder er det mer enn 25 kriminelle bander som selger løsepengevirusoperasjoner som en tjeneste (RaaS – Ransomware as a Service) globalt, så kommer de som kjører egne operasjoner (spesielt de mest avanserte som Ruyk, REvil, NetWalker, Ragnar Locker og Egregor), og deretter kommer alle de som kjøper tjenestene. En rask opptelling av de mest vanlige filtypene etter kryptering (hvert angrep/aktør merker krypterte filer ved å endre filtypen til noe særegent), viser ca. 200 forskjellige. Det sier litt om antall aktører der ute. Dessverre ser vi at utenlandske offentlige og private virksomheter betaler seg ut av slike hendelser, det finnes eksempler fra skoleverket i USA. Baltimore Public Schools med 115.000 studenter ble satt ut av spill ultimo november og betalte. Det samme gjorde det amerikanske helseforetak Universal Health Services og University of Vermont Health Network.

Crowdstrike - et amerikansk cybersikkerhetsselskap - melder i sin «2020 Global Security Attitude Survey» publisert 17. november 2020 at 27 % av de som rammes av løsepengevirus betaler. Det at så mange aktører betaler seg ut av løsepengevirus er foruroligende og fører til økt volum av slike angrep.

Selv om det ikke er kjent at noen kommune har vært utsatt for et vellykket løsepengevirusangrep av den nye typen, viser gjennomgangen her at dette er en stor trussel også for kommuner og fylkeskommuner og at konsekvensene kan bli veldig store. Det vil være katastrofalt for en kommune om kriminelle aktører begynner å presse brukere av psykiatriske- eller andre helsetjenester med innhold fra deres egne journaler. At aktører er villig til å gjøre dette, viser hendelsen fra Finland.

Tekniske dokumenter om kommuners infrastruktur ligger åpent på internett

Kommune-CSIRT ønsker i denne utgaven av *Situasjonsbilde* å sette søkelyset på en spesiell type informasjonspublisering. I forbindelse med offentlige anbudskonkurranser benyttes det anbudsportaler for å publisere dokumentasjon/spesifikasjon for anbudet. Norske kommuner og IKT-samarbeidsselskaper er pålagt å gjennomføre anbudskonkurranser via slike portaler. Kommune-CSIRT har ved flere tilfeller kommet over dokumenter og skisser som inneholder informasjon om IKT-infrastrukturer og vann-og-avløpsanlegg. Det være seg komplett dokumentasjon på IKT-infrastrukturer med routingtabeller, adgangslister og logisk infrastruktur. Beskrivelser av nødprosedyrer ved feil på infrastruktur, dokumentasjon på vannbehandlingsanlegg med tekniske tegninger, føringsveier og beskrivelse av nødprosedyrer ved beredskapssituasjon er også funnet.

Dette er typisk informasjon som kan anvendes av en ondsinnet aktør. Det kan også bidra til å svekke evnen til å kunne motstå uønskede hendelser i form av terror, sabotasje, hacking eller sosial manipulasjon.

Denne typen informasjon kan benyttes til å:

- Skaffe ondsinnede aktører tekniske veikart for bevegelse og spredning i virksomheten
- Avdekke svakheter i design og løsninger
- Avdekke rutiner
- Avdekke kritiske punkter med manglende redundans
- Vise programvareversjon og type utstyr
- Drive sosial manipulasjon for å tilegne seg tilgang både elektronisk og fysisk samt benyttes som grunnlag informasjonsutlevering hos kommune.

Kommunene må ha en plan for hvordan anbudsdokumenter som inneholder sensitiv informasjon skal håndteres og publiseres. Både at innholdet risikovurderes slik at det er avklart internt at denne informasjonen kan publiseres, men også at tilgangen til konkurransegrunnlaget begrenses. De som drifter anbudsportalene, har ingen mulighet til å sjekke om det som blir utlagt er skadelig eller kan misbrukes.

Lov om offentlige anskaffelser gir oppdragsgiver mulighet til å ettersende dokumentasjon til en tilbyder/leverandør på forespørsel. Leverandører er også underlagt taushetsplikt i forbindelse med konkurransen, noe som skal bidra til at informasjon ikke kommer på avveie.

Kommune-CSIRT varsler fortløpende kommuner som vi ser har denne typen informasjon offentliggjort.

E-postkontoer og passord på avveie

Som nevnt under «Hendelser» ble det i slutten av november publisert en fil på en rekke hacker forum som inneholder rundt 26000 hackede databaser med påloggingsinformasjon. Disse databasene inneholder totalt 226 884 000 unike epostkontoer, hvorav mange er nye og hittil ukjente lekkasjer. Disse skal etter alt å dømme stamme fra «sikkerhetsselskapet» Cit0day som har solgte tilgang til databaser med brukernavn og passord.

Kommune-CSIRT har analysert innholdet og databasene inneholder rundt 3600 kommunale epost-adresser.

Vi vet av erfaring at mange gjenbruker samme påloggingsinformasjon på både private og offentlige tjenester, samt på tjenester gjennom arbeidsgiver. Noen virksomheter har ikke iverksatt bruk av flerfaktorautentisering på de mest kritiske systemene. Samme påloggingsinformasjon kan derfor i noen tilfeller benyttes mot kommunal infrastruktur. Vi har varslet de berørte kommunene og driftsleverandørene slik at de får satt i gang tiltak for å forhindre eventuelt misbruk av påloggingsinformasjon.

Det er rapportert om at informasjon fra databasene benyttes i kampanjer for utsending av søppelpost. Passordene benyttes også i såkalt *credential stuffing* (bruk av kjent påloggingsinformasjon) og passordspray (bruk av kjente passord) mot en rekke tjenester for å se om de kan skaffe seg tilgang til tjenesten. Bruk av kjent påloggingsinformasjon var forøvrig en av angrepsmetodene som PST nevnte i sin pressemelding om angrepet på Stortinget i september.

Sikkerhetsbevissthet ved bruk av hjemmekontor

Gjennom denne rapporten har vi nå sett at det skjer en rekke cybersikkerhetshendelser mot både virksomheten og direkte mot den ansatte. Mange av de truslene man står ovenfor stiller krav til både den ansatte og virksomhetens IT-avdeling for å opprettholde samme sikkerhetsnivå som man har på kontoret.

Hjemmekontor er nesten blitt den nye normen for kontorarbeid etter utbruddet av pandemien, og det forventes at denne arbeidsformen delvis vil bli beholdt også etter at pandemien er over. Utstyr og infrastruktur som ikke er direkte IT-avdelingens ansvar – noe som ofte er tilfelle for hjemmekontor - har lett for å gå under radaren når det gjelder krav til cybersikkerhet og kontroll. Slikt utstyr og tjenester går inn under merkelappen Skygge-IT, og blir trukket fram som en av de større sikkerhetsutfordringene i dag.

Virksomhetens ledelse og sikkerhetsansvarlige har ofte ikke kontroll på eller prosedyrer for lagring i privat skykonto, lokalt utstyr som rutere, printere og andre datamaskiner, innsyn på skjerm og overhøring av samtaler osv. Med dette antyder vi at kommuneledelse og sikkerhetsansvarlig må stille strengere krav til hjemmekontor, som f.eks. forbud mot privat lagring, større grad av styrt / «managed» PCer med kun godkjente applikasjoner, krav til kontorets plassering og innsyn, internettilgang via arbeidsplassen (til VPN eller lignende - og så ut til internett for brannmurkontroll) og andre relevante tiltak.

Glasskula – hva ser vi komme?

Vi tror angrepene som beskrevet i denne rapporten, fortsetter i ukene og månedene fremover. Tema som vaksineringsprosess, COVID-19/Korona, stortingsvalg 2021 og andre store hendelser vil kunne utnyttes av ondsinnede aktører. Vi bør fremdeles være oppmerksomme på påvirkningsoperasjoner og falske nyheter gjennom sosiale medier og andre kilder, ikke minst når valgkampen blir mer intens.

Vi nevner spesielt vaksineringsprosess og involvering av virksomheter, myndigheter og privatpersoner i dette, fordi det er noe som vil oppta de samme gruppene de neste 6-12 månedene. Det har allerede blitt observert phishing-eposter til privatpersoner med vaksineringsinstruksjoner og registrering, inkludert et infisert skjemavedlegg i epost. Denne typen utnyttelse av en viktig hendelse med mye eksponering media, er en sannsynlig modus for svindlere de neste månedene.

Kompromitteringene av mot Sopra Steria, Synsam, Hurtigruten og andre virksomheter gir grunn til bekymring for vårt ansvarsområde. Vi ser at kommuner blir infisert av skadevare som har potensial for datatyveri og kryptering av filer med påfølgende utpressing og trussel om offentliggjøring, men de tilfellene vi har sett, har heldigvis resultert i annen utnyttelse - vanligvis utsendelse av nye spam/phishing-kampanjer. Vi tror likevel at kommuner eller fylkeskommuner vil bli rammet av den nevnte verste varianten, vi vet bare ikke når.

Vi tror at lekkasjer, sårbarheter og kompromitteringer på «Skygge-IT» vil øke i tiden fremover fordi stadig flere tar i bruk hjemmekontor, og fordi denne for mange vil bli en mer vanlig arbeidsform etter pandemien enn før. Dette innebærer at kommuneledelse og sikkerhetsansvarlig som nevnt må stille strengere krav til hjemmekontor og annet digitalt arbeid utenfor den tradisjonelle arbeidsplassen.

E-post vil fortsatt være den mest benyttede bæreren av skadevare og det blir fortsatt viktig å drive bevisstgjøring om digital sikkerhet i egen organisasjon.

Siste side

Rapportens aktuelle situasjonstips:

For brukere:
* Ha fokus på sikkerhet – ikke minst på hjemmekontoret
* Gjenbruk av brukernavn og passord er ingen god idé og bør unngås!
* Vær oppmerksom på COVID-19/Korona og vaksinerelatert phishing og spam

For driftspersonell:
* Foreta en risikovurdering med påfølgende tiltak for hjemmekontoret
* Oppgradér nettverkskomponenter som VPN, brannmur etc. så raskt som overhodet mulig!
* Gjennomfør tiltak som hindrer løsepengevirus (AppLocker, MS ATP, flertrinnsverifisering ++)

Relevante lenker:
Ny rapport fra Digitaliseringsdirektoratet om informasjonssikkerhet i kommunene:
https://www.digdir.no/informasjonssikkerhet/behov-styrke-informasjonssikkerheten-i-fylkeskommuner-og-kommuner/2128

Veileder til reglene om offentlige anskaffelser
https://www.regjeringen.no/no/dokumenter/veileder-offentlige-anskaffelser/id2581234/

Retningslinjer for sikkerhetstiltak ved elektronisk konkurransegjennomføring
https://www.regjeringen.no/contentassets/ae986b8264554cc2865ec09bd9e165f9/retningslinjer-for-sikkerhetstiltak-ved-elektronisk-konkurransegjennomforing---versjon-1.0.pdf

Kontakt Kommune-CSIRT: post@kommunecsirt.no eller telefon 90 85 00 42