DIGITALT SITUASJONSBILDE

Kommune-CSIRT

Rapport nr. 1 – 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 1. juli til 30. september.

Sammendrag

Dette er den første av en serie periodiske rapporter fra Kommune-CSIRT. Den har som ambisjon å dele et bilde av trusler, hendelser og sårbarheter som rammer eller kan ramme kommunesektoren.

Den siste tiden har både Stortinget og andre offentlige virksomheter blitt utsatt for omfattende dataangrep. Fellesnevneren er at epost-tjenestene er blitt angrepet og utnyttet.

Den 14. september, i et debattinnlegg på digi.no* skrev Kai Roer at sikkerhetskulturen i offentlig sektor er for dårlig. Kommune-CSIRT ser også utfordringer med sikkerhetskultur i kommunal sektor, og vil presisere:

> *Ansvaret for både digital sikkerhet, sikkerhetskultur og sikkerhetsbevissthet ligger hos virksomhetens ledelse! Dette er ikke noe som kan settes ut til underleverandører, driftsavdeling eller driftsselskap.*

Hendelseslisten vår for den rapporterte perioden viser at sårbarheter, gamle og nye, blir utnyttet. Dette er et faktum som dyktige sikkerhetsorganisasjoner er klar over, og de sørger for at åpningene for utnyttelse blir redusert til et minimum. Hendelsene viser at dette ofte glipper eller gjøres for sent hos offentlige virksomheter.

Angrepene mot offentlig sektor fortsetter i uforminsket styrke, både mot epostkontoer, internetteksponerte tjenester og hjemmekontorløsninger (VPN, Remote Desktop). Hensikten er både å tappe innloggingsdetaljer, kryptering av data for å drive med utpressing samt spionasje mot myndigheter.

Verden har de siste månedene sett en kraftig økning i antall aktører som har løsepengevirus i sin verktøykasse, både målrettede kampanjer og mer opportunistiske metoder («skyte med hagle») blir benyttet. I tillegg kommer trussel om publisering av stjålne data og salg til høystbydende, noe som øker alvorligheten i denne type angrep.

Når vi ser fremover, tror vi angrepene/hendelsene som beskrevet i denne rapporten, fortsetter. Tema som COVID-19, det amerikanske valget, norsk stortingsvalg og andre viktige hendelser vil kunne utnyttes av ondsinnede aktører. Vi bør også være oppmerksomme på påvirkningsoperasjoner gjennom sosiale medier og falske nyheter.

Nye digitaliseringsprosjekter: Vi tror også at angrepene mot nye digitaliserte tjenester vil øke. Kommunale prosjektledere og kommuneledelse må tenke sikkerhet samtidig som de tenker digitalisering. Når antall produkter, tjenester, funksjoner og sammenkoblinger øker, øker også sårbarheten og risikoen for sikkerhetsbrudd!

Hendelser

En skadevare har infisert flere små og mellomstore organisasjoner i helsesektoren
HelseCERT meldte i august om at en e-postkampanje med skadevare hadde infisert flere små og mellomstore organisasjoner i helsesektoren. Som et av sikkerhetstiltakene skrudde de på blokkering av makroer i e-post. I tillegg ble det bedt om at mistenkelige e-poster slettes. Skadevaren var kjent under navnet *Emotet*. Emotet er en skadevare som ofte spres ved hjelp av ondsinnede filer mottatt gjennom phishing. Den stjeler blant annet e-poster og bruker disse til å sende ut skadevare til nye mottakere som man har hatt e-postdialog med.

Kommuner angrepet av skadevare
Minst 10.000 personer i sju kommuner ble kvelden tirsdag den 1. september utsatt for et alvorlig e-postangrep. Det ble sendt e-poster til ansatte med vedlegg som inneholdt virus. E-postene var forkledd som e-poster fra kollegaer. Skadevaren som hadde infisert en datamaskin hos en av kommunene, var *Emotet* som nevnt i saken over.

IT-angrep mot Stortinget
1. september meldte Stortinget om at de var utsatt for et omfattende IT-angrep. Det ble registrert innbrudd på epost-kontoene til enkelte stortingsrepresentanter og ansatte. Etter analyser kunne Stortinget fastslå at det ble lastet ned ulike mengder data fra deres systemer. Arbeidet for å få et totalbilde på hendelsen og det potensielle skadeomfang er krevende, men mye tyder på at angriperne har utnyttet en svakhet i Microsoft Exchange epost-server.

Norfund svindlet for 100 millioner kroner
16. mars ble Norfund – en bistandsorganisasjon eid av utenriksdepartmentet – svindlet for 100 millioner kroner, men fordi svindlerne manipulerte kommunikasjonen mellom Norfund og låntager ble saken oppdaget først 30. april. Grunnen til at vi omtaler denne saken så lang tid i ettertid er fordi det først i juli forelå en grundig rapport fra PwC** om hendelsen. Det er mange læringspunkter å ta med seg fra denne hendelsen.

Svindlerne manipulerte og forfalsket informasjonsutveksling mellom Norfund og lånetager over tid på en måte som var realistisk i utforming, innhold og språkdrakt. Etter av uvedkommende kom på innsiden av e-postsystemet til Norfund kunne dokumenter og betalingsdetaljer forfalskes slik at 100 millioner kroner ble utbetalt til svindlere. PwC sin rapport viser at Norfund verken hadde flerfaktor autentisering eller kompetanse nok hos underleverandør til å oppdage og stoppe svindelen.

Norfund skal ha ros for sin åpenhet, både for egen beskrivelse og publisering av PwC-rapporten.

Dataangrep mot Sykehuset innlandet HF*
I august avdekket Sykehuspartner at en trusselaktør hadde gjennomført et angrep og kompromittert enkelte tjenester på internett som ble driftet av Sykehuset Innlandet HF. Sykehuspartner HF identifiserte sårbarhetene angriperen hadde utnyttet. Dette var en kombinasjon av en feilkonfigurert databaseserver og mangelfull inputvalidering i en tjeneste – en tjeneste som var gammel og dels basert på utdatert teknologi. Det var gjennom denne tjenesten angriperen fikk tilgang til data som lå i bakenforliggende databaser. Analyser viser at det er hentet ut data fra databasene.

Idrettsanlegg hacket
I august ble det avdekket at innloggingsdetaljer til en VPN-løsning for et idrettsanlegg var hacket og tilgjengelig på nettet. Anlegget tilhørte en kommune, og var drevet av et underliggende kommunalt selskap som ikke var en del av den kommunale IT-driften. Kommune-CSIRT varslet selskapet og løsningen

ble tatt ned og byttet ut. Løsningen hadde en sårbarhet som burde vært rettet et år tidligere. Manglende oppdateringsregime hos underleverandør fører til at dette sviktet.

Epost-kampanjene fra i vår fortsetter – nye kommuner rammet
I tillegg til Emotet-kampanjen i august, har norske kommuner erfart epost-kompromitteringer i stort omfang siden i vår. Brukernavn og passord blir hacket, så blir tilgangen solgt til aktører som vil kjøre phishing eller spam-kampanjer. Kampanjene kjøres gjerne midt på natta, og varierende mengde meldinger sendes ut. Aktørene benytter adresseboken på den hackede epostkontoen som mottagere. Dermed blir de ofte oppdaget siden mottager eller mottager-infrastruktur oppdager at det ikke er legitime meldinger. Likevel sprer det ofte seg videre. Tema for meldingene har vært blant annet «COVID-19 donasjoner» og «Oppgradering av epost» fra «IT-helpdesk».

Alvorlig digitalt angrep mot amerikanske sykehus, Universal Health Services (UHS) rammet
I de siste dagene i september – rapportert første gang 28.9 – meldte amerikanske nettaviser om at UHS ble rammet av løsepengevirus. Hendelsen påvirket tilgjengeligheten for hele datanettverket til virksomheten som har medisinske tjenester på over 400 lokasjoner og 92.000 ansatte. Hendelsen skjedde på søndag 26.9, og tre dager senere er systemene gradvis på vei opp igjen. Sikkerhetseksperter hevder at det sannsynligvis dreier seg om Ryuk ransomware, og at infeksjonen startet med en phishing-angrep. Ryuk benytter ofte Emotet som et verktøy i operasjonen.

Situasjonsbilde og vurderinger:

I offentlig sektor fortsetter angrepene i uforminsket styrke, både mot epostkontoer, internetteksponerte tjenester og mot hjemmekontorløsning (VPN, Remote Desktop). Hensikten er både å stjele innloggingsdetaljer, kryptering av data for å drive med utpressing samt spionasje mot myndigheter. Selv om Emotet-kampanjen tilsynelatende tok en kort pause i begynnelsen av september, ser den nå ut til å være revitalisert og kjører nye angrepsrunder med fornyet våpenarsenal og metoder. Årvåkenheten bør derfor holdes på et fortsatt høyt nivå.

Generelt har verden de siste månedene sett en kraftig økning i antall aktører som har løsepengevirus i sin verktøykasse, både målrettede kampanjer og mer opportunistiske metoder («skyte med hagle»). I tillegg er metodene mer utspekulerte da aktørene også stjeler data med trussel om publisering eller salg på det kriminelle markedet.

Omlegging til hjemmekontor har bidratt til økt sårbarhet. Det er minst to grunner til dette: for det første betyr det at mange virksomheter må opprette en ny tjeneste – adgang til virksomhetens IT-system hjemmefra – noe som i selv øker antallet mulige angrepsflater. I omleggingen kan det også bli behov for endring av epost-tjenesten – for eksempel flytting til Office 365. Da er det ikke alltid man får med seg alle sikkerhetsmekanismene man hadde i det gamle systemet inn i det nye. For det andre er hjemmeomgivelsene sjeldent preget av de samme sikkerhetsmekanismene som på kontoret. Det gir også en risiko for uønsket spredning av sensitive data, f.eks. via privat skylagring. Hvis det hjemme i større grad benyttes privat utstyr enn på jobb, øker risikoen ytterligere. Overgang til hjemmekontor medfører som regel høyere risiko for digital kompromittering og lekkasjer. Dette må ledelse og sikkerhetsansvarlige ta høyde for og innføre regler og tiltak som reduserer risiko.

Microsoft lanserte i september en rekke oppdateringer for sine produkter og kom samtidig med en klar anbefaling om å oppdatere systemene raskt for å fjerne sårbarheter. Samtidig er det lansert dokumentasjon på utnytting av flere av disse sårbarhetene. Det er derfor sannsynlig at en aktør ønsker å

utnytte disse sikkerhetshullene relativt raskt. Dette gjelder sentrale produkter som epost-server (Exchange), Office 365 og Active Directory.

NB! 14. september ble eksempelkode publisert som viser hvor enkelt det er å ta kontroll over Active Directory (AD) Controller ved å utnytte en spesiell sårbarhet i NetLogon (CVE-2020-1472), også kalt ZeroLogon. Rettelse/patch kom med patchetirsdag-pakken fra Microsoft i august. Til driftspersonell: Hvis denne sårbarheten ikke er patchet, gjør det snarest! Det er nå sett utnyttelse av sårbarheten av ondsinnede aktører. Alvorligheten understrekes av at amerikanske Department of Homeland Security 18. september pålegger alle føderale byråer og etater om å patche umiddelbart, og rapportere tilbake.

Konsekvenser for kommunens håndtering av kritiske situasjoner og hendelser
Kommune-CSIRT observerer hvordan enkelte kommuner rammes ekstra hardt ved digitale angrep når de samtidig er i en kritisk situasjon med håndtering av smittevern under COVID-19-utbrudd. Hvis den kanskje viktigste kommunikasjonskanalen - epost – sperres/tas ned, vil COVID-19 håndteringen lide kraftig. Prosesser for å håndtere slike samtidige krisesituasjoner/utfall, bør skrives inn i beredskapsplanverket til kommunen og drilles blant de ansatte og ansvarlige. Når et utfall av en kritisk tjeneste skjer, har man en plan for hvordan man opprettholder kommunikasjonen på best mulig måte.

Glasskula – hva ser vi?

Vi tror angrepene som beskrevet i denne rapporten, fortsetter i ukene og månedene fremover. Tema som COVID-19, det amerikanske valget, norsk stortingsvalg 2021 og andre store hendelser vil kunne utnyttes av ondsinnede aktører. Vi bør også være oppmerksomme på påvirkningsoperasjoner gjennom sosiale medier og falske nyheter, selv om disse kanskje ikke gir direkte konsekvenser for våre virksomheters operative drift. Det kan derimot påvirke samarbeid - både mellom kommuner og på tvers av forvaltningsnivåer, samt rokke ved integriteten og tilliten til lokale og sentrale myndigheter.

Over lengre tid har vi sett kampanjer som benytter Emotet, en skadevare som ofte spres ved hjelp av ondsinnede filer mottatt gjennom e-post-phishing. Vi er bekymret for disse kampanjene som sannsynligvis vil returnere i bølger. Emotet har i mange sammenhenger vært benyttet for å spre løsepengevirus og med såkalt "dobbel utpressing", som innebærer lekkasje/tyveri av sensitive data, kryptering av data og påfølgende trussel om publisering eller salg til andre kriminelle. Det har ikke blitt observert disse siste stadiene av Emotet-infeksjon i kommunesektoren etter vår informasjon, men vi bør absolutt være forberedt på at dette kan skje. Det er derfor ekstra viktig å beskytte sensitive data i tiden fremover.

Microsoft publiserte i september 120 oppdateringer til sine produkter, der 17 er å kategorisere som kritiske. De ga samtidig beskjed om at oppdateringene bør implementeres relativt raskt. Samtidig har sikkerhetsmiljøet publisert dokumentasjon på hvordan disse sårbarhetene kan utnyttes. Vi ser at flere aktører utnytter dette relativt raskt, ofte tar det kun dager etter publisering. Vi tror dessverre vi fortsatt vil se manglende oppdatering som årsak til kompromitteringer. Det er viktigere enn noen gang å ha et stramt oppdateringsregime.

Vi tror også at angrepene mot nye digitaliserte tjenester vil øke. Det er en eksplosiv økning i velferdsteknologi og automasjons- og IoT-installasjoner. Disse bør omfattes av sikkerhetsmekanismer på samme måte som annen digital infrastruktur i kommunen.

Kommunale prosjektledere og kommuneledelse må derfor tenke sikkerhet samtidig som de tenker digitalisering. Når antall produkter, tjenester, funksjoner og sammenkoblinger øker, øker også sårbarheten og risikoen for sikkerhetsbrudd!

Siste side

Rapportens aktuelle situasjonstips:

For brukere:

* Aldri klikk på lenker i epost-meldinger
* Aldri svar ja til aktivering av innhold i epost-vedlegg

Med mulig unntak av lenker og dokumenter du er helt trygg på, og som kommer fra en legitim kilde – men dobbeltsjekk!

For driftspersonell:

* Sørg for å patche kritiske komponenter så raskt som overhodet mulig!

Lenker:

*) https://www.digi.no/artikler/debatt-offentlige-virksomheter-ma-skjerpe-sikkerhetskulturen/499209
**) https://www.norfund.no/app/uploads/2020/07/Report_-Norfund-Independent-Assessment-of-the-LOLC-incident.pdf
***)https://sykehuset-innlandet.no/om-oss/aktuelt/nyheter/dataangrep-mot-sykehuset-innlandet-hf

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