DIGITALT SITUASJONSBILDE

Kommune-CSIRT

Rapport nr. 3 – 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 mai 2023 til oktober 2023.

Sammendrag

Mandag 23. oktober kunne vi i en nyhetssak på dn.no lese overskrifter som «Håndterer nytt avansert cyberangrep mot Norge», «Norge under angrep», «Går mot forsvarskommuner». Sjef for Nasjonal sikkerhetsmyndighet Sofie Nystrøm peker på at antallet svært avanserte cyberangrep mot Norge øker og at det er utfordringer for mange virksomheter knyttet til arbeidet med digital sikkerhet uten en betydelig bedret støtte.

> – De går mot viktige underleverandører, vi ser at kommuner spesielt med viktige beredskaps- og forsvarsinstallasjoner er i skuddlinjen og er svært sårbare. Så staten må bidra til å løfte cybersikkerhetsnivået kraftig fremover for å imøtegå det vi ser i trusselbildet. Det er en økning i svært sofistikerte cyberangrep mot Norge, sier Sofie Nystrøm.

Med dette som bakteppe og en økning i antall digitale sikkerhetshendelser presenterer Kommune-CSIRT på nytt et «Digitalt situasjonsbilde». Rapporten viser til hendelser som kan knyttes til offentlig forvaltning og type hendelser Kommune-CSIRT mener kan utgjøre en trussel mot kommunal sektor

I inn- og utland har det vært et økende antall tjenestenektangrep. Angrep har rammet internasjonale arrangement på politisk nivå og arrangørland. Her hjemme har det vært angrep mot både private og offentlige virksomheter som PST, Politiet, Avinor, finn.no og leverandører til nettsider for offentlige virksomheter.

I den siste perioden har man igjen sett flere ransomware-hendelser enn man har sett på lenge. Dette har for det meste rammet private virksomheter av forskjellig art. Tjenestenektangrep har fortsatt å ramme vesentlige aktører i samfunnet, og vi har sett at personopplysninger har blitt lekket ved overgang fra et gammelt til nytt system i en virksomhet.

I perioden har det også være flere utnyttelser av 0-dagssårbarheter. DSS-direktør Erik Hope var raskt ute og fortalte at de hadde avdekket en hittil ukjent sårbarhet i programvaren til en av deres leverandører. Denne alvorlige sårbarheten var utnyttet av en ukjent aktør, og i etterkant har man kunne lese at i minst to og en halv måned boret hackere seg inn i datasystemet som brukes av 12 norske departementer, og skadepotensialet for statssikkerheten er naturlig nok svært stort. I tillegg har man observert omfanget av MOVEit-saken (fildelingsløsning) og mot slutten av perioden har det også vært avdekket og utnyttet en alvorlig sårbarhet i Cisco sine ruterprodukter.

I denne sammenhengen er det naturlig at Kommune-CSIRT (og andre institusjoner) i sin analyse vurderer risiko for kompromittering ved digitale angrep som fortsatt høy. Vurderingen understøttes av en trend med økning av ulike typer cyberangrep, både kriminelle utpressingsangrep, tjenestenektangrep fra geopolitiske hacktivister og spionasje. I analysen beskriver vi også hvordan de kriminelle gruppene utvikler seg når det gjelder bruk av verktøy, organisatorisk og operasjonelt.

I denne utgavens TEMA har vi valgt å gi innspill til policyer som det finnes få konkrete råd rundt. Merkelig nok er passordpolicy og loggstrategi lite konkretisert hos betydningsfulle aktører som NIST og NSM. Her er det et udekket behov, og vi forsøker oss på å gi norske kommuner gode råd.

Hendelser

Omfattende cyberangrep på islandsk infrastruktur
I forkant av Europarådets toppmøte på Island som startet tirsdag 16. mai, var det en stor økning i forsøk på cyberangrep på islandsk infrastruktur. CERT-IS, det islandske cybersikkerhetsteamet, rapporterte om et uvanlig høyt antall dataangrep rettet mot islandske selskaper og institusjoner i oppkjøringen til Europarådets toppmøte i Reykjavik. Angrepene som var av typen tjenestenektangrep, fikk ingen alvorlige følger eller skader.

100-talls virksomheter offer for 0-dagssårbarhet
BBC, British Airways, Novia Scotia, PwC og EY var blant store navn på virksomheter som ble offer en 0-dagssårbarhet. Det utnyttede programmet, MOVEit, er mye brukt av bedrifter for å dele filer på en sikker måte. Morselskapet, Progress Software, varslet kunder om bruddet 31. mai og utstedte en oppdatering samtidig. Cybersikkerhetsforskere hevdet at hundrevis av selskaper til da kunne ha fått sensitive data i det stille eksfiltrert. Cl0p-ransomware-syndikatet kunngjorde på sine lekkasjesider på det mørke nettet sent tirsdag 6. juni at ofrene – som det ble antydet var hundrevis – hadde frist til 14. juni til å ta kontakt for å forhandle om løsepenger ellers ville de risikere å få sensitive stjålne data lagt ut åpent på nettet.

Trondheimsbedrift rammet av datainnbrudd
20. juni kunne man på virksomheten E.A. Smith sine nettsider lese at virksomheten var utsatt for et datainnbrudd. Med bakgrunn i datainnbruddet opplevde virksomheten driftsforstyrrelser hos Bygger´n og Smith Stål. Alle butikker og anlegg ble holdt åpne og det aller meste av transaksjoner gikk som normalt. Virksomheten ble etter hvert kontaktet med krav om løsepenger. Fra virksomheten ble det uttalt at det var uaktuelt å støtte opp om den typen kriminalitet ved å betale. Sikkerhetstjenester som følger med på det mørke nettet hevder at det var trusselaktøren ALPHV som stod bak angrepet og datalekkasjen. Aktøren tilhører gruppen med russiske kriminelle med knytninger til den nå avsluttede gruppen Conti og den fremdeles aktive Lockbit3.0

Flyktninghjelpen/NRC under dataangrep
Flyktninghjelpen (NRC) identifisert 13. juli et dataangrep på en nettbasert database som inneholdt personopplysninger til tusenvis av prosjektdeltakere. Så snart man ble oppmerksomme på bruddet, iverksatte man umiddelbare tiltak for å ta hånd om databasen for å beskytte personopplysningene og forhindre ytterligere skade. Cyberangrepet ble bekreftet å ha påvirket en frittstående nettsøknad for et enkelt program i en NRC-landsoperasjon. Det ble tatt skritt for å varsle og støtte berørte prosjektdeltakere, inkludert ved å sette opp en kontaktmulighet for folk for å få mer informasjon om saken.

Forsøk på leveranse av skadevare til norsk ambassade
14. juli kunne man lese på Digi.no at Russisk etterretning skal ha forsøkt å levere skadevare til Norges ambassade i Ukraina. En bruktbilannonse fra en tilsynelatende polsk diplomat ble benyttet som utgangspunkt. Hackere tilknyttet russisk etterretning skal ha forsøkt å angripe flere utenlandske diplomater i Kyiv med skadevare ved hjelp av en falsk bruktbilannonse. Norges ambassade i Kyiv skal ifølge Unit 42 ha vært en av utenriksstasjonene som ble forsøkt angrepet. Av over 80 ulike nasjoners utenriksstasjoner i Kyiv skal minst 22 ha blitt forsøkt angrepet av skadevaren, som både USA og Storbritannia mener stammer fra en av Russlands etterretningstjenester, SVR.

Tomra (panteautomatselskapet) utsatt for omfattende dataangrep
Panteselskapet Tomra ble mål for et omfattende dataangrep som direkte påvirket noen av selskapets systemer, skrev de i en børsmelding. Relevante myndigheter ble varslet og alle tilgjengelige ressurser ble satt til å stanse angrepet som ble oppdaget søndag morgen 16. juli. Tomra koblet umiddelbart fra noen

systemer for å begrense angrepet samtidig som de undersøkte om kunder eller ansatte opplevde redusert stabilitet.

Tolv departementer utsatt for dataangrep
24. juli: Departementenes sikkerhets- og serviceorganisasjon (DSS) avdekket et dataangrep på IKT-plattformen til tolv departementer. – Dette er en påminnelse om at cybertrusselen er høyst reell og er en betydelig del av den nye sikkerhetspolitiske situasjonen vi lever i, sa kommunal- og distriktsminister Sigbjørn Gjelsvik (Sp) på en pressekonferanse. DSS-direktør Erik Hope var raskt ute og fortalte at de hadde avdekket en hittil ukjent sårbarhet i programvaren til en av deres leverandører. Denne sårbarheten var utnyttet av en ukjent aktør. De hadde på det tidspunktet lukket sårbarheten.

Cybersecurity and Infrastructure Security Agency (CISA) i USA og Norwegian National Cyber Security Center (NCSC-NO) hos Nasjonal sikkerhetsmyndighet ga ut en felles Cybersecurity Advisory (CSA) som svar på den aktive utnyttelsen hos DSS av CVE-2023-35078 og CVE-2023-35081.

I etterkant har man kunnet lese at i minst to og en halv måned boret hackere seg inn i datasystemet som brukes av 12 norske departementer. Det kommer frem i en rapport fra Nasjonal sikkerhetsmyndighet (NSM). Den kom en drøy uke etter at regjeringen 24. juli varslet om det alvorlige dataangrepet.

Schibsted-aviser, finn.no, Politiet og PST rammet av tjenestenektangrep
Flere av politiets nettsider, Schibsted-aviser og annonsetjenesten Finn.no ble 27. juli utsatt for dataangrep. Tjenestenektangrep førte for flere av aktørene til fullstendig nedetid på nettsiden og videre ustabilitet etter at nettsidene var oppe igjen. For PST sin del påvirket ikke angrepet deres interne nettverk og datasystemer. - Problemene lå hos en ekstern leverandør og det har påvirket vår hjemmeside, skrev PST på pst.no.

Personopplysninger feilaktig publisert på kommunens nettside
Trondheim kommune skriver i en pressemelding at feilen oppsto i overgangen til et nytt saksbehandlingssystem i slutten av juli. Personopplysningene ble liggende ute i 16 timer mellom 31. juli og 1. august. Kommunen oppdaget selv feilen. 17 personer anses å være berørt av sikkerhetsbruddet, skriver kommunen. Datatilsynet er varslet om hendelsen, og kommunen ville videre ta kontakt med de som var rammet.

Svensk virksomhet utsatt for Akira ransomware
8. august kunne man lese at Räddningstjänsten Västra Blekinge hadde blitt utsatt for ransomware. Denne redningstjenesten er en svensk kommuneforening med tre medlemskommuner: Karlshamn, Olofström og Sölvesborg. *Akira* – trusselaktøren som sannsynligvis står bak angrepet - hevder at siden disse foreningene ikke er interessert i å beskytte sine borgerdata, vil de laste opp alt de har om dette selskapet på sine nettsider/lekkasjenettsted på det mørke nettet.

Avinors nettsider nede på grunn av hackerangrep
Avinor sine nettsider er nede etter at deres server er blitt hacket, opplyste pressevakt Cathrine Framholt til VG. En planlagt oppgradering den 16. august gikk ikke som den skulle. Problemene fortsatte utover neste dag, og på et tidspunkt ble nettsiden hacket. Avinor informerte utad om at dette førte til at deres nettsider er nede, men at alle flytider, bookinger og personlig informasjon lå på andre servere, så det var kun nettsiden som var berørt.

Nedetid på en rekke kommunale nettsider over hele landet
Nettsider til en rekke kommuner over hele landet var nede eller ustabile kvelden torsdag 17. og utover formiddagen fredag 18. august på grunn av et dataangrep. Acos leverer nettjenester til en rekke kommuner og fylkeskommuner. Bent Inge Storheim, daglig leder i Acos, uttalte at de hadde en pågående

hendelse som de undersøkte, men at det på ettermiddagen samme dag så ut som de kommunale nettsidene var tilgjengelige igjen. DDoS-angrep mot en av våre kunder har fått konsekvenser for flere, sier Storheim. Angrepet rammet Acos samt deres underleverandør Advania (tidligere Visolit og Telecomputing), som tilbyder av datasentertjenester. Acos er en betydelig leverandør til kommunal sektor og på sine nettsider viser de til avtaler med 260 kommuner.

Molde kommune utsatt for «bounty hunter»
Samtidig som det var ustabilitet og nedetid på en rekke kommunale nettsider, mottok Molde kommune torsdag kveld 17. august, klokken 19.45 en «e-post fra mulig angriper som ønsket penger for å rette opp i problemet». Daglig leder Fred Gjørtz i ROR-IKT (interkommunalt IT-foretak for Aukra, Hustadvika, Molde, Rauma og Vestnes) fortalte til Digi.no at det er en person, en såkalt «bounty hunter», som mener å ha funnet en svakhet og som henvendte seg med ønske om å motta belønning. Dusørjegeren skal ha skrevet på engelsk med ønske om premiering for å ha varslet om en svakhet i en tredjepartsløsning kommunen har brukt. Ved en tilfeldighet skjer dette akkurat samtidig som nettsidene tok telling, mener IKT-foretaket. – Vi kan ikke se noen sammenheng mellom den svakheten og tjenestenektangrepet, sammenfatter Gjørtz til nettavisen.

Flere norske virksomheter rammet av dataangrep - Oslo kommunes nettsider var nede
22. august. Et tjenestenektangrep mot Stortingets nettsider ble registrert tirsdag formiddag av IT- og sikkerhetsavdelingen. Oslo kommune meldte også samme dag at deres nettsider var «midlertidig utilgjengelig». Hackergruppen NoName057 har nok en gang rettet seg mot Norge. De tok på seg ansvaret for DDoS-angrepet mot ni organisasjoner i Norge, inkludert både offentlige g private organisasjoner. Disse var BPS Nord, Ferde AS, Ruter AS, Boreal Norge AS, Agder Kollektivtrafikk, Stortinget, Skipsverft, BaneNor Log, og Oslo kommune. På sin Telegram-kanal listet NoName057(16) ofrene og delte check-host-lenker for å bevise suksessen til de påståtte DDoS-angrepene, og sa følgende: "Vi har effektivt lammet Norges nettsteder."

Qakbot-nettverket tatt ned
FBI, det amerikanske justisdepartementet og byråer i Frankrike, Tyskland, Nederland, Storbritannia, Romania og Latvia skrev tirsdag 29. august at de hadde stengt ned Qakbots botnet (infisert datamaskinnettverk). I tillegg hadde de også proaktivt fjernet skadelig programvare fra infiserte enheter. Qakbot malware har blitt brukt siden 2008 for å infisere mer enn 700 000 enheter rundt om i verden og tillot et bredt utvalg av nettkriminelle å starte løsepenge-angrep så vel som svindel.

Trygg-Hansa - personopplysninger åpent tilgjengelig på nett.
Gjennom å bytte ut noen sifre i URL-en, kunne kunder av forsikringsselskapet åpne andre kunders dokumenter. 650.000 kunder av forsikringsselskapet har hatt sine personopplysninger åpent tilgjengelig på nett. Integritetsskyddsmyndigheten (IMY), Sveriges svar på Datatilsynet, skriver i en pressemelding: - Dokumentene som har vært tilgjengelige for uvedkommende inneholdt i visse tilfeller sensitive personopplysninger, blant annet opplysninger om helse med høyt detaljnivå. I etterkant av dette har det svenske forsikringsselskapet fått en bot på 35. millioner svenske kroner fra IMY, som mener at problemet var så grunnleggende at Trygg-Hansa burde ha oppdaget det allerede før systemet ble innført. Problemet varte fra oktober 2018 til februar 2021, og eksponerte personnumre, økonomisk informasjon, kontaktinformasjon og helseopplysninger.

Abacus IT rammet av løsepengevirus
Abacus IT meldte mandag formiddag den 25. sept. om at de hadde en «alvorlig sikkerhetshendelse» i sitt driftssenter. Til Digi.no fortalte selskapet at -kunder som kjører et IT-system eller tjeneste fra Abacus IT datasenter, var i en eller annen form rammet. Abacus IT er et selskap som blant annet leverer skyløsninger for store og små bedrifter deriblant kommuner. Selskapet tilbyr også en rekke løsninger fra Visma, og har også egen nettbutikk for datautstyr for bedriftskunder.

Inventum - Leveradør av IT-tjenester hacket
Et rørleggerfirma på Gjøvik kan ha tapt opp mot ti millioner kroner etter at deres leverandør av IT-tjenester ble hacket. Tirsdag morgen 3. oktober oppdaget ansatte i firmaet Knut Malmberg AS at datasystemer firmaet er avhengig av ikke fungerte. Etter hvert ble det klart at deres IT-leverandør Inventum Øst var utsatt for et dataangrep. Over en uke etter angrepet var systemene fremdeles ikke i funksjon igjen. Erland Lekang, daglig leder i Inventum Øst bekreftet overfor NRK.no at de var utsatt for et dataangrep og at de ble nødt til å ta ned deler av deres datatjeneste. Nøyaktig hvor mange virksomheter som var rammet var usikkert, men det var snakk om en kundemasse på 20-30 virksomheter. 20. oktober ble det offentliggjort informasjon om at aktøren Akira sto bak angrepet på Inventum Øst.

IKM-gruppen utsatt for utpressingsforsøk
Det norske konsernet IKM Gruppen bekrefter til NRK at de har blitt utsatt for et utpressingsforsøk. Til NRK.no 11. oktober uttalte konsernsjef Ståle Kyllingstad: - I dag er det ingen økonomisk skade. Når det kommer til data på avveie så vet vi det ikke. Vi har valgt å verken snakke med eller å betale noe som helst. Kyllingstad forteller at de har et desentralisert IT-system og at det bare er en mindre del av den engelske virksomheten deres i Aberdeen som ble rammet. – Vi var oppe og gikk allerede etter 24 timer. Vi har gode backup-systemer så selskapsdriften går helt fint, sier Kyllingstad. I etterkant har det vist seg at det trolig er aktøren ALPHV som sto bak angrepet.

Alvorlig sårbarhet avdekket i Ciscos nettverksprodukter
Mandag 16. oktober rapporterte Cisco om en kritisk 0-dagssårbarhet i webgrensesnittet (web UI) til IOS XE-programvaren, som aktivt utnyttes av trusselaktører for å installere fjernadgangsverktøy (RATs) og bakdør på sårbare enheter som er eksponert på internett. Sårbarheten gjør det mulig for en angriper uten autentisering å opprette en høyt privilegert konto på den berørte nettverksenheten for å få full kontroll og utføre vilkårlige kommandoer. Cisco IOS XE-programvaren brukes på flere av Ciscos mye brukte bedriftsnettverksenheter, som svitsjer og rutere.

Tirsdag 17. oktober utførte forskere ved VulnCheck en internett-skanning og identifiserte over 10 000 kompromitterte Cisco IOS XE-systemer som hadde blitt infisert med RAT av ukjente trusselaktører. Senere ble det avdekket enda flere kompromitterte systemer, men etter noen dager ble antallet sterkt redusert fordi hackerne hadde endret bakdøren. Det er indikasjoner på at flere enheter i Norge er infisert, og noen av disse kan være tilknyttet kommuner. Angripere med denne typen ubegrenset fjernadgang til en nettverksenhet kan utføre følgende handlinger med tilknyttede konsekvenser:

- Overvåke nettverkstrafikk – avlytte privilegert nettverkskommunikasjon.
- Innsette og omdirigere nettverkstrafikk – utsette bedriften for "man-in-the-middle"-angrep.
- Bryte seg inn i beskyttede nettverkssegmenter.

Situasjonsbilde og aktuelle tema:

Risikovurdering høsten 2023: Trusselbildet er fortsatt alvorlig

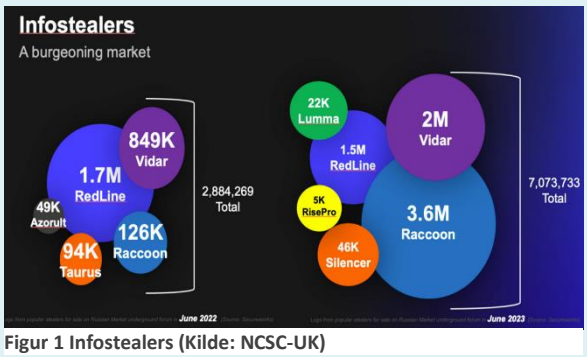
Situasjonsbildet og sårbarheter

Siden forrige situasjonsbilde i juni har trusselbildet utviklet seg i forskjellige retninger. Stikkord er mer profesjonalisme og større bruk av opportunistiske kampanjer blant de mest avanserte kriminelle. Det er også observert en økt bruk av såkalte «infostealer»-skadevare som igjen fører til et økt tilbud av informasjonspakker (logindetaljer, systeminfo, m.m.) på de kriminelle markedsplassene. Dette, kombinert med kritiske sårbarheter i sentrale løsninger som Citrix Netscaler og MoveIT fildeling, har medført økt risiko for norske kommuner. Spesielt Citrix-sårbarheten gjorde kommuner med denne løsningen mer utsatt, og flere ble utsatt for kompromitteringsforsøk. I oktober ble nok en kritisk sårbarhet avdekket og raskt utnyttet av trusselaktører. Denne gangen en svakhet i Cisco IOS XE som muliggjorde uautorisert tilgang til nettverksutstyr (rutere, svitsjer m.m.) gjennom Web-grensnittet til boksene.

Profesjonalisering og verktøy

For at avanserte kriminelle grupper skal overleve i konkurransen, må de ha tillit hos sine partnere og underleverandører. Deres egen operative sikkerhet må også ha høy kvalitet, og de må ha tilstrekkelig teknisk kompetanse til å utføre operasjonene. Feiler de på noen av disse områdene, forsvinner de raskt fra «bransjen» og trusselbildet. Derfor er det relativt stor utskifting og 'rebranding' av kriminelle aktører. De som klarer å holde seg i 'bransjen' over lengre tid, har derfor høyere profesjonalitet enn resten. Eksempler på slike aktører er Cl0p, som fant nulldagssårbarheten i MoveIT og gjennomførte i sommer hundrevis av vellykkede kompromitteringer. Cl0p har også bak seg angrep mot vannforsyning, noe de selv har uttalt vil være et prioritert område fremover og er derfor en alvorlig trussel mot norske kommuner. Den andre trusselaktøren som bør nevnes er Lockbit, som er en spinoff av Conti da den gruppen ble delt opp i fjor. Lockbit er svært aktiv, og lekket informasjon på det mørke nettet om ca. 20 utpressingsofre per uke de første ukene i september. Begge aktørene er basert i Russland, med mulige forgreninger til andre eks-sovjetstater. Å bli rammet av digitale angrep fra disse aktørene er derfor noe av det mest alvorlige en kommune kan bli utsatt for.

For et par år siden var såkalt Big Game Hunting i skuddet. Trusselaktørene fant da globale selskaper med høy omsetning, og startet en målrettet kampanje mot disse. Et eksempel her kan være Hydro-angrepet. Etter hvert som sikkerheten har blitt bedre hos mange store selskaper, og fordi slike angrep er krevende når det gjelder forberedende arbeid, er trenden nå at man skyter mot alt og alle, og ser hvor man kommer seg inn og får fotfeste. Så kjører man videre med digital utpressing, eller selger tilgangen til andre kriminelle hvis man ikke ønsker å gjennomføre et angrep selv. I tillegg dukker det opp nye verdikjeder, forsterkede salgskanaler og utbredelse av sofistikerte verktøy. En type verktøy eller skadevare som effektiv henter ut innloggingsdata og annen informasjon fra infiserte datamaskiner og som vi ser økt bruk av, er såkalte «infostealers». Dette er skadevare som infiserer datamaskinen f.eks. via nettfisking på epost, og etter installasjonen samler den informasjon fra tastetrykk, logindetaljer i browser og annen anvendelig informasjon. Informasjonen sendes så via internett hjem til de som står bak skadevaren/nettfiskingen. Da har man informasjonspakker som kan selges på det mørke nettet eller andre markedsplasser eller kriminelle partnere. Infostealere som «Vidar»



Figur 1 Infostealers (Kilde: NCSC-UK)

og «Racoon» har økt svært mye siste året, og de kriminelle markedsplassene flommer nærmest over av informasjonspakker derfra.

Trusler og risikovurdering
Trusselaktørenes utnyttelse av Citrix- og MoveIT-sårbarhetene har påvirket norske kommuner både direkte og indirekte. MoveIT mest indirekte, da leverandører til kommuner ble rammet. Noen kommuner erfarte forsøk på og delvis kompromittering av sin Citrix NetScaler-løsning.

Reaksjonen på disse truslene bør være økt årvåkenhet og rask oppdatering for å fjerne sårbarheter.

Vi har også de siste månedene observert tjenestenektangrep mot norske online-tjenester, og noen av angrepene har gått ut over tilgjengeligheten på kommune online-tjenester. Sistnevnte skjedde da offentlige tjenester som ble hostet av Advania (tidligere Visolit i Norge), ble angrepet. Det gikk utover tjenester fra ACOS som mange kommuner benytter. Slike tjenestenektangrep får derfor ofte følgefeil og indirekte påfører andre virksomheter utilgjengelighet for sine tjenester. Norske kommuner må være forberedt på at deres tjenester kan bli skadelidende ved slike angrep.

Denne høsten ser vi også en tydelig økning av aktivitet fra ransomware-aktører globalt, men også mot norske offentlige og private virksomheter er trykket høyt.

De mest vanlige inngangsvektorene for digitale angrep er nettfisking fra e-post, logindetaljer på avveie og sårbare tjenester som er eksponert mot internett. For mottiltak se siste side i denne rapporten.

Hovedvurdering
På bakgrunn av hevnangrep mot norske online-tjenester, kompromitteringer muliggjort av kritiske sårbarheter i sentrale produkter, og det generelle trykket mot vestlige lands offentlighet, vurderer vi risikonivået uforandret fra våren 2023, og man bør fortsatt være årvåkne og sørge for best mulig sikring av kommunenes og fylkeskommunenes digitale systemer.

Kommune-CSIRT anser fortsatt digitale angrep med dobbel utpressing fra avanserte, organiserte kriminelle som den største trusselen mot norske kommuner og fylkeskommuner.

TEMA: Anbefalinger for passord og logging

Vi mottar ofte spørsmål om anbefalinger rundt sikkerhetstiltak, for eksempel hvor langt tilbake i tid bør man ha logger, hva slags passordpolicy anbefales etc. Det er stor etterspørsel etter gode, konkrete råd her, og verken NSM eller internasjonale institusjoner er klare på f.eks. passordlengde eller logglengde bakover i tid.

I denne utgaven av *Digitalt Situasjonsbilde* tar vi for oss nettopp disse to policyene, og våre konkrete anbefalinger.

Loggepolicy:
Med logger mener K-CSIRT brannmurlogger, systemlogger, weblogger, AD-logger, skylogger og andre logger som kan gi innsikt i hvordan trusselaktører har kommet seg inn og operert i systemet.

*K-CSIRT anbefaler at man tar vare på logger i minimum **6 måneder, og anbefalt 12 måneder**.*

Grunnen til at vi anbefaler minimum 6 måneder, er tidligere erfaringer med kompromitteringer. Avanserte kriminelle og fremmed etterretning kommer ofte på innsiden av offerets nettverk uker og måneder før selve det avsluttende angrepet finner sted. Et eksempel på avsluttende angrep er datakryptering ved ransomwareangrep. Hvis man mangler logger for det tidspunktet man ble initialt kompromittert, er det vanskeligere å avdekke hvordan dette skjedde. Det gjør det komplisert for forsvarerne å bygge et system som hindrer ny kompromittering etter gjenoppretting. Vi vil også legge til at det er viktig å logge all autentisering, bevegelse, privilegiumendringer, nedlastinger, opplastinger og endringer av sikkerhetsoppsett. Vi har sett eksempler på at kun avviste påloggingsforsøk logges, men ikke suksessfulle påloggingen. Det er en type konfigurasjon som gjør stadfestelsen av inngangsvektor i beste fall usikker, i verste fall umulig å bestemme.

Passordpolicy:
Microsoft sin passordpolicy for Office365 består av lengdekrav, kompleksitet og byttefrekvens. Standard krav er minimum 8 tegn, 3 av 4 tegntyper (tall, små og store bokstaver, spesialtegn) må være med. Byttefrekvens er satt opp til ca. hver 3. måned (90 dager). Lengden på 8 tegn er etter vår mening altfor kort. Hvis det er mulig å bruke 'Brute Force' hacking av passord mot kontoen, tar det under et sekund å knekke dette.

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2023

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

HIVE SYSTEMS
› Learn how we made this table at hivesystems.io/password

Plansjen som viser tid det tar for å hacke ulike lengder og kompleksitet og som er laget av Hive Systems, må kun ses på som en illustrasjon på forskjellen på ulike lengder. Selve tallene gir selvsagt en indikasjon, men er ikke absolutte. Tiden det tar vil være avhengig av mange faktorer, regnekraft, nettverkskapasitet, oppdagelsesfare m.m.

Vår anbefaling:
Minimum 12 tegn, anbefalt 16. Ved bruk av 16 tegn snakker vi om svært mange år for å hacke passordet.

Ingen krav til kompleksitet, ren tekst er ofte lettere å huske enn utropstegn og hash. Forskere mener dessuten at brukere ved full kompleksitet lager egen systematikk som er lett å knekke.

Byttefrekvens: **Intet periodisk bytte, kun ved mistanke om kompromittering**, eller alternativt en gang hver 12. måned. Dette er også begrunnet med den uheldige tendensen med å lage systemer av passordsekvenser.

Forutsetningen her er selvsagt at systemene tillater denne policyen. Det er det ikke alle som gjør, og man må da gjøre det beste ut av det og benytte de kravene som kan benyttes. For framtidige anskaffelser kan man også vurdere å ta med krav om fleksibel og kundebestemt passordpolicy i systemkravene.

Glasskula – hva ser vi komme?

Mer ransomwareangrep
Når vi kikker inn i glasskula, ser vi fortsatt dobbel utpressing med eller uten kryptering som er kontinuerlig trussel, kanskje også noe økende mot jul og neste år. Opportunismen hos de kriminelle vil øke, da dette konseptet viser seg å gi mer avkastning for de kriminelle enn målretting mot store selskaper. Profesjonaliteten og «darwininismen» i aktørfloraen gjør at de beste og mest avanserte overlever – og blir dermed vanskeligere å beskytte seg mot.

Mer spionasje
Vi vurderer det også som sannsynlig at digital spionasje vil øke fremover ettersom krigene i Midt-Østen og Ukraina utvikler seg. Når det gjelder krigen i Midt-Østen som representerer en endring i sikkerhetsbildet, er det flere avanserte aktører i regionen, og både Israel og Iran er har vist både kapasitet og evne til kompromittering av andre lands informasjonssystemer og å hente ut viktige data. Det gjelder både informasjon om og fra involverte parter i Midt-Østen, men også støttespillere i vestlige land.

Kunstig intelligens – flere bruksområder for trusselaktørene
I glasskula forrige gang nevnte vi perfekte phishing e-poster og 'Social Engineering' som bruksområder for KI av avanserte trusselaktører og som vi vurderer vil øke i omfang fremover.

Dette er fortsatt meget aktuelt, men vi kan fylle på den listen over sannsynlig bruksområder fremover med:

- Data mining og eksfiltrering. Identifisering av verdifulle data kan gjøres under kompromittering ved hjelp av KI, og eksfiltrering kan gjøre selve overføringen med lavere deteksjonsmulighet
- Utvikle mer sofistikert skadevare og mer målrettet ransomware
- Spredning av skadevare ved hjelp KI-genererte YouTube-videoer
- Tjenestenektangrep – mer dynamiske angrepsmønstre basert på overvåking og analyse
- Oppdagelse og utnyttelse av nulldagssårbarheter basert på tidligere sårbarhetskunnskap og smart testing
- Forbedrede unnvikelsesteknikker i skadevare. Mye skadevare har teknikker for å unngå å bli oppdaget, og disse kan vesentlig forbedres gjennom bruk av KI.

Siste side

Rapportens aktuelle situasjonstips:

Sikkerhetskultur og operasjonell sikkerhet – for vanlige brukere:

- Ikke aktiver innhold i vedlegg og ikke klikk på lenker verken i Teams, e-post 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 god passord- og loggepolicy (se egen temaartikkel)
- Sørg for å ha sikkerhetskopier som er reelt offline, og testet for gjenoppretting
- Patch/oppgrader alle IT- og OT-løsninger så raskt det lar seg gjøre - angrepene mot disse øker
- Ikke la utrangert utstyr bli stående eksponert mot internett
- Gjennomfør ekstra sikkerhetssjekk på tekniske installasjoner, VA og SD-anlegg.

Relevante rapporter, dokumenter og kampanjer lansert i perioden:

Nasjonal sikkerhetsmyndighet: «Nasjonalt digitalt risikobilde 2023»: https://nsm.no/getfile.php/1313382-1697777843/NSM/Filer/Dokumenter/Rapporter/Nasjonalt%20digitalt%20risikobilde%202023.pdf

Politiet – KRIPOS: «Generativ kunstig intelligens og cyberkriminalitet»: https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/etterretningsrapport-generativ-kunstig-intelligens---kripos.pdf

Nasjonal sikkerhetsmyndighet: «Konseptvalgutredning for en nasjonal skytjeneste»: https://nsm.no/regelverk-og-hjelp/rapporter/konseptvalgutredning-for-nasjonal-skytjeneste

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.**