DIGITALT SITUASJONSBILDE

Kommune-CSIRT

Rapport nr. 2 – 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 februar 2023 til mai 2023.

Sammendrag

I forrige situasjonsbilde omtalte vi fjoråret som et år hvor antallet alvorlige kompromitteringer mot kommuner og fylkeskommuner gikk merkbart ned. Så smalt det i Nord-Norge i begynnelsen av februar. Flere kommuner ble angrepet, og det var både ulike metoder som ble benyttet og forskjellige trusselaktører som stod bak. En kommune ble angrepet av en trusselaktør som utnyttet manglende oppdatering av lokal epost-server for å komme på innsiden, mens andre ble offer for at leverandører til kommunene hadde blitt frastjålet innloggingsdata som kunne brukes mot de samme kommunene. Trusselaktørene kunne logge inn, og gjorde det! Heldigvis hadde kommunene mekanismer som medførte at de kriminelle ikke klarte å ta over systemene, og ble etter hvert kastet ut og systemene herdet. Da den uønskede innloggingen fant sted, var det ikke aktivert multifaktorautentisering på kontoene. Innloggingsdata var lagt ut for salg på det mørke nettet.

Under perioden dette situasjonsbildet gjelder for, har vi ved flere anledninger sett at norske offentlig virksomheter har vært utsatt for distribuert tjenestenektangrep/DDoS-angrep. I lys av Ukraina-krigen og varslene om hevnangrep mot norske online-tjenester var ikke disse angrepene mot eksempelvis NSM og SSB uventet. Dette er noe vi antagelig vil se igjen i tiden som kommer. Hendelsene mot Målselv- og Vadsø kommune er nevnt, og senere i februar ble også en annen norsk kommune rammet av dataangrep. Angivelig skal dette ha vært en tilsvarende hendelse som rammet Målselv kommune. Igjen viser dette at norske kommuner ikke er fredet for vellykkede cyberangrep.

I tillegg til hendelser innenlands har vi også sett en rekke hendelser i utlandet som mulig kan treffe norske kommuner. Dette gjelder angrep mot vannforsyningsanlegg og ikke minst angrep mot helseinstitusjoner. Ved en gjennomgang av hendelsene kan man også se at et cyberangrep skapte utfordringer for Visma Recruit og offentligjobb.se i Sverige. Dette gjorde at kommuner innenfor et tidsvindu ikke kunne gjennomføre ansettelsesprosesser på en normal måte. Denne hendelsen er en pekepinn på hvor viktig det er for norske kommuner å følge opp leverandører og gjennom kontrakter sørge for at det stilles krav til digital sikkerhet innenfor tilgangsstyring til eller fra kommunen og i systemer kommunen benytter fra en tredjepart.

Digitale systemer rundt oss består av programvare, kode. Millioner av kodelinjer. Kode er lett å endre, men programmering er også en profesjon hvor det er fort gjort å gjøre feil. I tillegg skal applikasjoner og løsninger snakke sammen, og utveksle data via såkalte grensesnitt eller grenseflater. Disse grenseflatene kan også bli sårbare. For å rette opp i programvare og forbedre den, må man oppgradere, oppdatere eller patche programvaren når feil og svakheter avdekkes. Med dette som grunnlag er hovedtema for situasjonsbildet «Hvorfor er patching og oppgradering så viktig?».

I glasskulen vil vi knytte noen betraktninger til kunstig intelligens som et svært aktuelt tema for tiden. Vi vil også kort være innom andre tema som Cybercrime as a Service, hevnagrep for Ukraina-støtte samt offerspesialisering hos trusselaktørene.

I lys av Ukraina-krigen, hevnangrep mot norske online-tjenester, forsvarets hevede beredskap, det generelle trykket mot vestlige lands offentlighet og de siste angrepsforsøkene mot nord-norske kommuner, vurderer vi risikonivået uforandret fra i fjor/årsskiftet, og man bør fortsatt være årvåkne og sørge for best mulig sikring av kommunenes og fylkeskommunenes digitale systemer.

Hendelser

Kunstig intelligens brukes til å utvikle skadevare
Sikkerhetsselskapet Check Point Research (CPR) rapporterer i februar i år at de har oppdaget ondsinnede aktører som benytter ChatGPT til å utvikle skadevare. CPR-forskere fant nylig et tilfelle av cyberkriminelle som brukte ChatGPT til å «forbedre» koden til en infostealer-skadevare fra 2019, skriver sikkerhetsselskapet. Infostealer er navnet på en type trojaner som er designet for å hente ut data fra ofrenes systemer. Sikkerhetsselskapet fant også eksempler på at ChatGPT ble brukt til å skrive kode, basert på kommandoer som spesifiserte skadevarens ønskede funksjonalitet – som for eksempel å stjele en bestemt type filer.

SAS utsatt for cyberangrep
Flere SAS-kunder opplevde tirsdag 14 februar å bli logget inn på andres profiler og få tilgang til andre brukeres bonuspoeng, flyvninger og persondata. SAS sin nettside var også nede. Det er uklart hvor lenge, men VG ble gjort oppmerksom på feilen like etter klokken 17. Rundt klokken 19 samme dag var den oppe og gikk igjen. Tidligere tirsdag gikk hackergruppen «Anonymous Sudan» ut og hevdet at de sto bak et omfattende angrep på flere svenske nettsider, og viste til koranbrenningen i Sverige. Sveriges Television var blant nettsidene som ble rammet.

SVT og andre svenske institusjoner utsatt for cyberangrep
Sveriges nasjonale TV-kringkastingsselskap SVT ble tirsdag 14. februar rammet av brudd på tjenester etter en serie nettangrep som gjorde deres nettsted utilgjengelig. Dette skjedde etter at universiteter, sykehus og regionale administrasjonskontorer møtte lignende angrep uken før. Ifølge SVT kunne det dreie seg om et tjenestenekt-angrep – et angrep på et datasystem som, selv om det ikke forårsaker permanent skade eller gir tilgang til hemmelig informasjon, kan bidra til store forstyrrelser ved å hindre bruken av systemet.

Fauske kommune utsatt for datainnbrudd
Onsdag 22. februar måtte Fauske kommune stenge ned all trafikk på nett etter at det ble avdekket et innbrudd utenfra i deres datasystemer. Leder for innovasjon og utvikling i Fauske kommune, Tom Erik Holteng, bekreftet at kommunen var blitt utsatt for et datainnbrudd ovenfor Saltenposten. Holteng informerte kommunestyret samme uke at det ikke var noe som tydet på at informasjon er på avveie, men at de likevel valgte å stenge ned all trafikk til kommunens servere onsdag. Det ble uttalt fra kommunen at angrepet hadde likheter med angrepet Målselv kommune ble utsatt for tidligere i mnd. Et angrep Kommune-CSIRT omtalte i forrige «Digitale Situasjonsbilde».

Danske sykehus utsatt for dataangrep
Hjemmesidene til flere sykehus i Region Hovedstaden var nede ettermiddagen søndag 26 februar. Søndag kveld var nettsidene oppe igjen. Anonymous Sudan skriver på Telegram at nettsidene ble angrepet på grunn av koranbrenninger. De skriver at flere nettsider kommer til å bli rammet.
Region Hovedstaden bekreftet på Twitter at nettsidene var nede, men skrev ikke hva som vår årsaken. De skrev samtidig at den digitale infrastrukturen ellers ikke var påvirket. Samme hackergruppe hevdet å stå bak et dataangrep mot den svenske kringkasteren SVT tidligere i februar. Også da sa gruppen at koranbrenninger var årsaken til angrepet.

NSM bekrefter dataangrep mot norske virksomheter
Nasjonal sikkerhetsmyndighet (NSM) bekreftet torsdag formiddag 2. mars at de var kjent med tjenestenektangrep mot norske virksomheter eksempelvis egne nettsider og nettsidene til SSB. – Nettsidene kan oppleves trege og utilgjengelige. Denne type angrep handler gjerne om å få oppmerksomhet og synlighet, snarere enn å påføre skade, sier pressevakt Marit Hverven til Dagbladet.

Hverven sa videre at NSM kjenner til hvem som står bak, men ønsker ikke å uttale seg om dette. Hun vil heller ikke si noe om størrelse på angrepet.

Skadevaren Emotet er tilbake etter tre måneders pause
Emotet malware-operasjonen spammet igjen ondsinnede e-poster fra tirsdag 7. mars etter en tre måneders pause. Nettverket er gjenoppbygget og infiserer igjen enheter over hele verden. Emotet er en beryktet skadelig programvare distribuert via e-post som inneholder ondsinnede Microsoft Word- og Excel-dokumentvedlegg. Når brukere åpner disse dokumentene og makroer blir aktivert, vil Emotet-kode bli lastet ned og inn i minnet.

Angrep mot NSM og SSB sine nettsider
Nettsidene til Nasjonal sikkerhetsmyndighet var nede tirsdag morgen 14. mars. Klokken 10.00 er sidene oppe igjen. Nettsidene til Nasjonal sikkerhetsmyndighet (NSM) ble tatt ned tirsdag formiddag grunnet et pågående tjenestenektangrep mot flere virksomheter. Som NSM tidligere påpekte, så må vi regne med flere slike dataangrep. Denne type angrep handler gjerne om oppmerksomhet snarere enn å påføre skade, skrev fagdirektør Andreas Skjøld-Lorange. Også SSBs (Statistisk sentralbyrå) nettsider var nede tirsdag morgen.

Dataangrep på vannforsyning hos fylkesavdelingen i Geauga(US)
Onsdag 12. april, rundt klokken 04.00, begynte et sikkerhetsprodukt kalt CrowdStrike Falcon å legge merke til mulige ondartet skript og kommandolinjeaktivitet på en kritisk server for vannforsyning. Kort tid før klokken 08.00 begynte ansatte innen teknisk analyse å motta en serie alvorlige høyprioriterte varsler gjennom deres Cybersecurity Center, fra CrowdStrike, som indikerte det som så ut til å være et betydelig og vedvarende angrep på denne serveren for vannforsyning. CrowdStrike blokkerte automatisk tilgangen til serveren og satte i gang en rekke prosedyrer og instruksjoner for ytterligere å isolere og beskytte fylkets nettverksinfrastruktur.

Cyberangrep skapte utfordringer for Visma Recruit og offentligjobb.se
28. april rapporterte CERT.se om driftsforstyrrelser i rekrutteringssystemet til Visma og offentligjobb.se. Systemet var nede i flere dager – flere kommuner og myndigheter ble berørt. Blant annet Enköping kommune og selskapet har rapportert hendelsen til den svenske personvernmyndigheten (IMY). I etterkant er det uttalt i media at forstyrrelsene skyltes et hackerangrep mot Visma sin driftsleverandør. En av konsekvensene av angrepet var at det ikke var mulig å søke kommunale jobber på den vanlige måten. Totalt var det et hundretalls av Visma sine kunder, både offentlige og private, som ble påvirket av hendelsen.

Ransomwareangrep mot Politiet i Dallas (US)
Styret i Dallas bekreftet at et løsepenge-angrep kompromitterte en rekke servere i deres systemer, inkludert Dallas Police Department sitt nettsted. Sent mandag morgen den 1. mai. rapporterte J.D. Miles fra CBS News Texas at strømbruddet påvirket avdelingens dataassisterte utsendelsessystem, kalt CAD, som dirigerer politiet til nødsituasjoner og andre samtaler. Problemet tvang mottakere av 911-anrop til å manuelt skrive ned meldinger og de var kun i stand til å svare gjennom telefoner og radioer. CBS News Texas skaffet et bilde av løsepengevarenotatet. Hackerne, en gruppe kalt Royal, hevdet at de krypterte byens kritiske data, og truet med å legge ut sensitiv informasjon på nettet. Royal har også angrepet norske virksomheter.

FBI har beslaglagt 13 domenenavn knyttet til distribusjon av DDoS-for-hire-services
FBI beslagla i mai 13 domenenavn knyttet til stresstjenester på nettet som lar betalende kunder leie og starte ødeleggende, distribuerte tjenestenektangrep mot måldomener/tjenester (DDoS-angrep - Distributed Denial-of-Service). Ti av domenene er gjenoppstått fra DDoS-for-hire-tjenester som FBI

beslagla i desember 2022, da ble seks amerikanske menn siktet for datakriminalitet for angivelig å ha brukt denne typen tjenester.

Det multinasjonale teknologiselskapet ABB rammet av Black Basta løsepengevirus
11. mai kunne vi lese at ABB hadde vært utsatt for et Black Basta ransomware-angrep. Det sveitsiske multinasjonale selskapet ABB er en ledende leverandør av elektrifiserings- og automatiseringsteknologi. ABB har hovedkontor i Zürich, Sveits, og sysselsetter omtrent 105 000 ansatte og har 29,4 milliarder dollar i omsetning for 2022. Som en del av tjenestene sine utvikler selskapet industrielle kontrollsystemer (ICS) og SCADA-systemer for produksjon og energileverandører. For norske kommuner leverer ABB i størst grad systemer innen vann og avløp.

SAS´ nettsider i Norge, Sverige og Danmark nede etter Cyberangrep
02. juni var SAS sine nettsider helt eller delvis utilgjengelig fra morgenen av. Det var også utfordringer med SAS-appen. I sosiale medier skriver Anonymous Sudan at de står bak hackerangrepet på SAS sine nettsider, noe de også har gjort tidligere, blant annet da nettsidene var nede sist uke. Hackergruppen skriver at de krever 10 millioner dollar av SAS. Ut fra etterarbeidet etter angrep på SAS i februarhar flere hevdet at det er russiske Killnet som står bak Anonymous Sudan, eller at de er en del av et større nettverk der Killnet har en vesentlig rolle.

Situasjonsbilde og aktuelle tema:

Situasjonsbilde – heftig oppstart av 2023

I forrige situasjonsbilde omtalte vi fjoråret som et år hvor antallet alvorlige kompromitteringer mot kommuner og fylkeskommuner gikk merkbart ned. Så smalt det i Nord-Norge i begynnelsen av februar. Flere kommuner ble angrepet, og det var både ulike metoder som ble benyttet og forskjellige trusselaktører som stod bak. En kommune ble angrepet av en aktør som utnyttet manglende oppdatering av lokal epost-server for å komme på innsiden, mens andre ble offer for at leverandører til kommunene hadde blitt frastjålet innloggingsdata som kunne brukes mot de samme kommunene. Trusselaktørene kunne logge inn, og gjorde det! Heldigvis hadde kommunene mekanismer som medførte at de kriminelle ikke klarte å ta over systemene, og ble etter hvert kastet ut og systemene herdet. Da den uønskede innloggingen fant sted, var det ikke satt på multifaktorautentisering på kontoene. Innloggingsdata var lagt ut for salg på det mørke nettet.

Hendelsene over understreker betydningen av gode rutiner og policy for IT-drift. I hvert eneste Digitale Situasjonsbilde har vi poengtert viktigheten av oppdatering/patching og MFA. Det er vanskelig å forstå at disse prinsippene og rutinene fremdeles enten er ikke-eksisterende eller mangelfullt fulgt opp. Det er observasjoner og kunnskap som tyder på at det har vært en angrepsbølge mot nord-norske kommuner. Hendelsene over viser sannsynligvis at det som skal til for at mange kommuner blir kompromittert, er at de mer avanserte trusselaktørene viser økt interesse for norske kommuner og retter angrepene mot disse. Dette understrekes av informasjon fra andre vestlige land som opplever en jevn strøm av angrep og kompromitteringer av offentlige tjenester. Mest rammet av angrep mot offentlig sektor de siste månedene er USA, Canada, Tyskland, Frankrike og Italia.

Når det gjelder viktige teknologiske begivenheter i 2023, så er kunstig intelligens (KI) et aktuelt tema med flere nyvinninger. Mest interessant er chat-botene (ChatGPT, Bard) som kan løse eksamensoppgaver, skrive utredninger og utføre programmeringsoppgaver på bestilling. Som en av hendelsene våre omtaler, så har også trusselaktørene oppdaget nytten med denne teknologien. Som mottiltak forsøker de som tilbyr KI-tjenester å avsløre og nekte ondsinnet bruk av teknologien, men det finnes som vanlig metoder for å komme rundt disse tiltakene. Utviklingen av KI har pågått i mange år, og grunnlagsdataene til disse nye tjenestene har også vært tilgjengelig på nettet i lang tid. Det nye nå er de avanserte språkmodellene og evnen til å sette sammen både innhold, form og bilder/lyd på en troverdig og språklig elegant måte.

Hovedvurdering
I lys av Ukraina-krigen, hevnangrep mot norske online-tjenester, forsvarets hevede beredskap, det generelle trykket mot vestlige lands offentlighet og de siste angrepsforsøkene mot nord-norske kommuner, vurderer vi risikonivået uforandret fra i fjor/årsskiftet, 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: Hvorfor er patching og oppgradering så viktig?

Digitale systemer rundt oss består av programvare, kode. Millioner av kodelinjer. Kode er lett å endre, men programmering er også en profesjon hvor det er fort gjort å gjøre feil. I tillegg skal applikasjoner og løsninger snakke sammen, og utveksle data via såkalte grenseflater eller grensesnitt. Disse grenseflatene kan også bli sårbare. For å rette opp i programvare og forbedre den, må man oppgradere, oppdatere eller patche programvaren etter hvert som feil og svakheter avdekkes. Som oftest brukes benevnelsen oppdatering eller patching.

Figur 1: Oppdatering av programvare (Illustrasjon: Kaseya)

Å holde applikasjonene sine oppdaterte kan virke som en ubetydelig oppgave i en travel hverdag, men det er likevel et skritt som er avgjørende for å sikre både din digitale trygghet og applikasjonens optimale funksjon. Det er som et pulserende hjerte i en moderne teknologidrevet verden – hvis det stopper, kan det få alvorlige konsekvenser.

Å holde applikasjoner oppdatert er en investering i sikkerheten og brukeropplevelsen. Når utviklere oppdager sikkerhetshull eller feil i programvaren, frigir de oppdateringer for å rette opp i problemene og beskytte brukerne. Ved å ignorere disse oppdateringene, setter man seg selv og sine digitale eiendeler i fare. Hackere og ondsinnede aktører kan utnytte kjente sårbarheter i utdatert programvare for å få tilgang til sensitiv informasjon, eller i verste fall, ta kontroll over systemet ditt.

I tillegg til å beskytte brukerne mot sikkerhetstrusler, inneholder programvareoppdateringer ofte forbedringer i ytelse og funksjonalitet. Utviklere jobber kontinuerlig med å forbedre applikasjonene sine, og å holde seg oppdatert betyr at man får glede av disse forbedringene.

Fra et sikkerhetsmessig ståsted er patching viktig for alle tjenester, men spesielt viktig for de som er tilgjengelige via internett da disse er mer utsatt. Tetting av sikkerhetshull og sårbarheter er en viktig grunn til å patche systemer og holde dem oppdatert. Nye sikkerhetstrusler og sårbarheter oppdages kontinuerlig, og patching er en måte å beskytte mot disse truslene. Uten patching kan tjenesten, koden eller grenseflaten bli utsatt for angrep som kan resultere i tap av sensitiv informasjon, ødeleggelse av data, fysiske skader og i verste fall tap av liv. Internett er grenseløst, og ondsinnede angripere vil til enhver tid forsøke å trenge seg inn i virksomheters digital løsninger.

For eksponerte tjenester er det spesielt viktig å patche jevnlig da angripere målrettet går mot disse - gjerne med bruk av automasjon og kjente utnyttbare sårbarheter, så vel som nulldagssårbarheter (en nulldagssårbarhet er feil som det foreløpig ikke finnes rettelse/patch/oppdatering for). En internetteksponert tjeneste har flere tilgjengelige angrepsvektorer (angrepsvektor er fagsjargong for angrepsmetoder) og er dermed mer sårbare for angrep.

I tillegg kan patching være et krav for å overholde forskrifter og lover. Eksempelvis kan en tjeneste som håndterer personlig identifiserbar informasjon være pålagt å overholde kravene i personvernlovgivning / GDPR, og regelmessig patching kan være nødvendig for å sikre at dette overholdes. Datatilsynet har nylig

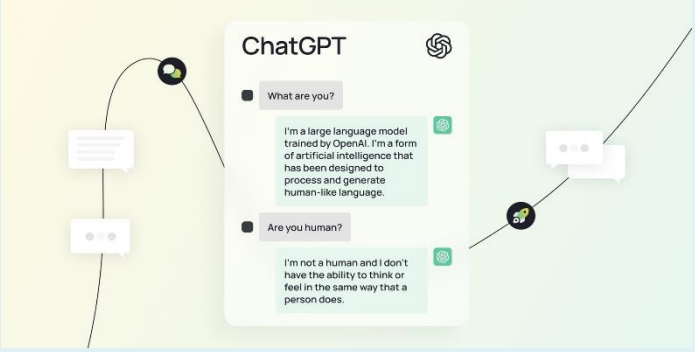
satt i gang en prosess med tilsyn hos opp mot 100 kommuner, hvor etterlevelse av personvernlovgivning er i fokus.

Oppdatering/patching har i enkelte tilfeller også medført spredning av skadevare eller innebygd kode som åpner bakdører for ondsinnede aktører. Dette kalles ofte leverandørkjedeangrep. To eksempler her er SolarWinds overvåkingssystem som ble hacket hos produsenten, og det ukrainske regnskapssystemet M.E.Doc som ble hacket og infisert av kampanjen NotPetya. Førstnevnte medførte at russisk etterretning skaffet seg en bakdør hos viktige kunder som f.eks. det amerikanske forsvarsdepartementet og kunne tappe informasjon derfra. Det andre eksempelet medførte blant annet et tap for det danske fraktselskapet MAERSK på 2 milliarder kroner.

Likevel er dette eksempler som bekrefter unntaket. Samlet sett er patching viktig for å beskytte alle digitale tjenester og sikre at de fungerer optimalt og sikkert.

I en kommune må ledelsen og IT-ansvarlige ha et bevisst og fremoverlent forhold til styring av patche-processen, såkalt «patch management».

Skrevet av Stig Mosand, Bjørn T. Tveiten og ChatGPT (Kunstig Intelligensstyrt samtalerobot)



Figur 2: Hva er ChatGPT (Kilde: Ultimate.ai)

Oppgave: Finn ut hvilke avsnitt som er skrevet av ChatGPT i teksten over. Det er en fin øvelse i å kunne avsløre KI/AI-generert innhold. Send svaret til post@kommunecsirt.no

NB! Teksten fra ChatGPT er verifisert av Kommune-CSIRT, så vi står inne for også den delen.

Glasskula – hva ser vi komme?

Cybercrime as a Service
Når vi kikker inn i glasskula, ser vi nye kriminelle tjenester som tilbys, og som vi vurderer som økende i tiden som kommer. En av disse er «Cybercrime as a Service» (CaaS) hvor metoder, verktøy og infrastruktur leveres av erfarne kriminelle teknikere, og pakken kan kjøpes av kriminelle som verken har kompetanse, infrastruktur eller verktøy. Ofte er avtalen en prosentandel av svindelinntektene. Flere og flere kriminelle ser på cybercrime som en lettvint og nærmest risikofri vei til mye penger. Denne typen tjenester kan sees på som en mer generell og kanskje foredlet utgave av «Ransomware as a Service» (RaaS) som har eksistert et par år. Disse verdikjedene/leverandørkjedene vil trekke enda flere kriminelle til disse miljøene, og flere kriminelle betyr vanligvis flere angrep.

Hevnagrep for Ukraina-støtte
Vi vurderer det også som sannsynlig at hevnangrep mot norske digitale tjenester vil fortsette ut 2023. Hevnen utføres av russiske hacktivister og er basert på Norges støtte til Ukraina. Angrepene vil for det meste være av typen distribuerte tjenestenektangrep, men også andre og kanskje mer fordekte og farlige angrep vil kunne forekomme.

Offer-spesialisering
En annen trend i cybercrime ser ut til å være mer spesialisering hos trusselaktørene - spesielt når det gjelder valg av ofre. Det er en viss trend at de som angriper utdanningsinstitusjoner holder seg til denne sektoren, det samme er observert innenfor sykehus og lignende virksomheter. Noen har også lært seg vannforsyning og angriper disse fordi de kjenner til hvordan de er satt opp og driftes. Denne spesialiseringen vil resultere i flere vellykkede angrep i tiden som kommer.

Kunstig intelligens
I glasskula ser vi også at ondsinnede aktører i større grad vil ta i bruk kunstig intelligens (KI) som verktøy for sine cyberoperasjoner. KI har allerede vært i bruk en god stund av sikkerhetsleverandører med eksempelvis maskinlæring og anomalideteksjon i nettverkssensorer, og på trusselaktørsiden i form av såkalt «deep fake» forfalskninger av video og lyd.

De nye intelligente chatbotene – eller mer presist den teknologien som ligger under - kan og vil bli brukt til å lage tilnærmet perfekte phishing e-poster, utføre sosiale undersøkelser forut for digitalt angrep (social engineering) og lage tekst for påvirkningsoperasjoner. Dette kan gjøres takket være den avanserte språkteknologien som er utviklet kombinert med smart uthenting og filtrering av allerede eksisterende informasjon på nettet. Alt som er falskt kan gjøres mer troverdig med KI! Det gjelder også generering av falske bilder, lyder og videoer.

Det er også sannsynlig at KI vil bli bedre til å finne sårbarheter i programvare enn tradisjonelle verktøy, men dette har uansett vært en trend over lengre tid og tilbys i dag av sikkerhetsleverandører som innbakt teknologi i sine løsninger. Noen er bekymret for at kriminelle som ikke kan IT, vil bruke den nye teknologien til å lage skadevare. Vi deler ikke den bekymringen, i hvert fall ikke som dagsaktuell trussel. Teknologien kan brukes av programmerere til å forbedre eksisterende programvare, men ikke til å lage velfungerende, funksjonelle og feilfrie programmer på oppdrag av ikke-programmerere.

Siste side

Rapportens aktuelle situasjonstips:

Sikkerhetskultur og operasjonell sikkerhet – for vanlige brukere:

- Ikke aktiver innhold i vedlegg og ikke klikk på lenker verken i epost eller SMS (uten å dobbeltsjekke med avsender)
- Aktiver multifaktorautentisering der du kan.
- Gjenbruk av brukernavn og passord er ingen god idé og må unngås!

De viktigste sikkerhetstiltakene – for drifts- og sikkerhetsavdelingen:

- Sørg for multifaktorautentisering for *all* tilgang utenfra
- Sørg for å ha sikkerhetskopier som er reelt offline, og testet for gjenoppretting
- 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: Sikkerhetsfaglig råd – Et motstandsdyktig Norge.
https://nsm.no/getfile.php/1312994-1683615611/NSM/Filer/Dokumenter/Rapporter/Sikkerhetsfaglig%20r%C3%A5d%20-%20Et%20motstandsdyktig%20Norge.pdf

Politiet - Kripos: Cyberkriminalitet 2023 – Politiets årlige temarapport om kriminalitet mot datasystemer og kriminalitet støttet av datasystemer.
https://www.politiet.no/globalassets/04-aktuelt-tall-og-fakta/datakriminalitet/cyberkriminalitet-2023.pdf

Regjeringen.no – NOU 2023:17 - Når er det alvor, Rustet for en usikker fremtid.
https://www.regjeringen.no/contentassets/4b9ba57bebae44d2bebfc845ff6cd5f5/no/pdfs/nou20232023 0017000dddpdfs.pdf

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.**