DIGITALT SITUASJONSBILDE

Kommune-CSIRT

Rapport nr. 2 – 2021

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

Sammendrag

Siden siste rapport (publisert i april) har det vært en rekke utpressingsvareangrep (ransomware / løsepengevirus) mot både private og offentlige virksomheter i inn- og utland. Spesielt vil vi trekke frem Volue som ble rammet av utpressingsvareangrep, identifisert som skadevaren Ryuk, i begynnelsen av mai. Volue er leverandør av programvare til kraftselskap, vann og avløpsetater og annen kritisk infrastruktur. For opp mot 100 norske kommuner fikk dette angrepet konsekvenser knyttet til tjenester innen vann og avløp.

Utpressingsvareangrep har vi i perioden også sett mot selskapet Nordlo i Haugesund. En av de berørte virksomhetene var Vakt og Alarm AS som har om lag 250 kommuner som kunder. Ifølge Vakt og Alarm ble konsekvensen av hendelsen noe nedsatt funksjonalitet i tjenestene som selskapet leverer til norske kommuner. Datasenteret til Axiell Norge (tidligere Bibliotekenes IT-senter) ble også rammet av et dataangrep av samme type som Nordlo. Tjenester de leverer til en rekke norske bibliotek og skoler ble utilgjengelig.

Videre kan det nevnes store hendelser som utpressingsvareangrep mot virksomheten som drifter USA's største drivstoffrørledning, Colonial PipeLine, skandinaviske GK-gruppen, Accenture, Inocean og Kaseya. Dette viser stor aktivitet fra aktører som benytter utpressingsvare, og ved angrepet på sistnevnte virksomhet, en programvareleverandør, ble om lag 60 direkte-kunder og om lag 1500 kunder av kunder rammet. En av virksomhetene som ble rammet hardt var Coop Sverige.

Kommune-CSIRT la stor vekt på utpressingsvareangrep i forrige situasjonsbilde og gjør det også denne gang. Angrep, aktører og offersammensetning for løsepengeangrep utvikler seg stadig. Noen aktører er nærmest forsvunnet, andre har blitt tatt av politiet og nye har kommet til.

I lys av å være en konstant trussel mot norske kommuner, har vi denne gangen Business Email Compromise (BEC) som et eget tema under «Situasjonsbilde og vurderinger». BEC er en svindelkategori som retter seg mot nær sagt alle typer virksomheter som gjennomfører bankoverføringer. Bedrifts- eller offentlig tilgjengelige e-postkontoer til ledere eller nøkkelpersonell innen eksempelvis økonomi blir gjerne forfalsket eller kompromittert. Informasjonen eller kontoene blir så benyttet for å utføre eller få en person til å utføre pengeoverføringer. I tema-artikkelen beskriver vi BEC, hvordan dette benyttes og hvordan man best kan beskytte seg mot en slik type svindel.

I tiden fremover vil vi fortsatt trekke frem avanserte løsepengeangrep med dobbel utpressing som den største trusselen. Proaktivt sikkerhetsarbeid mot denne trusselen er viktig for norske kommuner. Kontoovertakelser ser vi mye av, og vi frykter en økning i BEC-svindel mot kommuner gjennom ulike typer svindelkampanjer hvor kriminelle ved hjelp av e-post, Facebook eller andre virkemidler får kontroll over kommunale brukerkontoer, eksempelvis på Microsoft 365. Kampanjer som benytter falske Facebook-kontoer kombinert med SMS for å lure til seg tilgang til e-post-kontoer, er et av mange, ferske eksempler.

Hendelser

Nye saker for Q2/Q3

Kompromitterte e-postkontoer
I perioden denne rapporten tar for seg har det vært flere hendelser hvor det har blitt oppdaget kompromitterte brukerkontoer som er blitt benyttet for å sende ut svindel-e-post. Dog kan det ut fra rapporteringer til K-CSIRT se ut som det har vært en liten nedgang denne perioden mot de to foregående.

Cyberangrep slo ut sykesignalanlegg i flere norske kommuner
Torsdag 22. april ble det oppdaget et dataangrep mot selskapet Nordlo i Haugesund. En rekke virksomheter ble berørt og en av dem var alarm-, kommunikasjon- og trygghetsløsningsleverandøren Vakt og Alarm. Vakt og alarm har om lag 250 kommuner som kunder og leverer i hovedsak trygghetsalarmer, men også noen alarmmottakssystemer. Ifølge Vakt og alarm ble ikke backupsystemene deres rammet av viruset, men en konsekvens ble noe nedsatt funksjonalitet i en periode for tjenestene selskapet leverer til norske kommuner.

Flubot treffer Norge
Mot slutten av april mottok mange nordmenn tekstmeldinger på engelsk om å hente en tilsendt pakke. Dersom en lar seg lure og følger lenken fra en Android-mobil, leder den til en nedlastingsside for malware. For å installere skadevaren må brukeren slå på muligheten for å installere apper fra ukjente kilder og svare ja til flere sikkerhetsadvarsler. Det er malwaren Flubot som blir installert, og denne vil laste ned personlige detaljer og prøve å lure brukeren til å gi fra seg nettbank-detaljer. Flubot vil også fortsette å sende SMS-meldingene videre til brukerens kontakter. Hittil har heldigvis Flubot hatt begrenset spredning i Norge, muligens fordi få Android-brukere i Norge benytter seg av tredjeparts app-butikker. (Telenor TSOC Blogg)

DDoS-angrep mot den belgiske regjeringen
Det meste av den belgiske regjeringens IT-nettverk gikk ned etter et massivt DDoS-angrep. Internettforbindelsen og interne systemer samt offentlige nettsteder ble tatt ut. Angrepet var rettet mot Belnet, en ISP som er finansiert av myndighetene og som tilbyr internettforbindelse for belgiske regjeringsorganisasjoner, som parlamentet, utdanningsinstitusjoner, departementer og forskningssentre. Hendelsen påvirket aktiviteten til mer enn 200 belgiske regjeringsorganisasjoner. Påvirkede tjenester inkluderte regjeringens offisielle skatte- og skjemaarkivportal, men også IT-systemer som brukes av skoler og universiteter for fjernundervisning. Dette skjedde rett forut for en behandling av Kinas håndtering av uigur-minoriteten i det belgiske parlamentet. Angrepet medførte at saken ikke ble behandlet.

Den belgiske regjeringen har i tillegg vært kompromittert av Hafnium siden 2019.
Belgiske regjeringsansatte fortalte at hackere brøt seg inn i nettverket til innenriksdepartementet i en sikkerhetshendelse som fant sted i april 2019. Innbruddet ble oppdaget i mars i år mens regjeringens IT-ansatte undersøkte statusen til Exchange-e-postserverne etter at Microsoft advarte kunder om angrep fra en kinesisk hackergruppe som de kaller Hafnium. Ansatte fant Exchange-servere som var sårbare og trengte oppdatering, men IT-personalet ved Federal Public Service Interior - landets innenriksdepartement - fant også flere tegn på kompromitteringer som var datert år tilbake, snarere enn måneder da de første Hafnium-angrepene ble oppdaget.

Volue rammet av dataangrep
Onsdag 5. mai meldte Volue, en leverandør av programvare og online tjenester til kraftselskap, vann og avløpsetater og annen kritisk infrastruktur, at de hadde blitt rammet av et målrettet dataangrep. Angrepet ble satt i gang ved 22-tiden tirsdag 4. mai, da et løsepengevirus/kryptovirus, identifisert som skadevaren Ryuk, begynte å kryptere og ødelegge filer. Volue rapporterte kort tid etter hendelsen at det ikke ble observert tegn til at opplysninger var stjålet eller kopiert ut, men Volue kunne ikke si dette med sikkerhet. De kunne ikke avkrefte at persondata var på avveie. For mange norske kommuner fikk dette angrepet en rekke konsekvenser. Nært opp mot 100 kommuner benytter Volue som leverandør av tjenester til vann og avløp. En rekke tjenester fra Volue ble utilgjengelig, og daglig drift med behov for data levert gjennom disse tjenestene stoppet delvis opp.

Løsepengeangrep mot virksomheten som drifter USA's største drivstoffrørledning
Fredag 7. mai tok et løsepengeangrep ned virksomheten rundt den største drivstoffrørledningen i USA - Colonial Pipeline med 2,5 millioner fat per dag med bensin og annet raffinert drivstoff. Rørledningen går fra raffinerier i Texas til destinasjoner i hele det østlige USA. Dette er den største påvirkningen et cyberangrep har hatt på fysisk drift ved kritisk infrastruktur i USAs historie. Flere rapporter tilskriver angrepet en kriminell gruppe kalt "DarkSide", kjent for løsepengeangrep. En fersk rapport fra Cybereason anslår at gruppen har gått målrettet mot godt over 40 ofre, med løsepengekrav som varierer fra $ 200 000 til $ 2 millioner dollar per hendelse. Det spekuleres i at fotfeste er oppnådd ved at det er benyttet phishing- eller spear-phishing-angrep designet for å stjele påloggingsinformasjon eller for å aktivere skadelig programvare i e-postvedlegg eller ved annen nedlastning av en skadevare.

Svenske Folkhälsomyndigheten forsøkt hacket
Databasen SmiNet som benyttes for å lagre innmeldinger om smittsomme sykdommer ble stengt ned etter forsøk på hacking. SmiNet lagrer elektroniske rapporter om smittsomme sykdommer som er underlagt varsling i henhold til svensk lov om smittsomme sykdommer, for eksempel covid-19. Det svenske folkehelsebyrået har oppdaget at det har vært flere innbruddsforsøk i SmiNet-databasen.

15.000 e-poster forsøkt sendt ut fra kommunal e-postkonto
I juni ble over 15.000 e-post forsøkt sendt ut fra en kommunal e-postkonto tilhørende Tromsø kommune. E-posten inneholdt et dokument med lenke til en falsk innloggingsside med kommunens logo på. Ut fra vurderinger kommunen selv gjorde antar de at det var brukernavn og passord de kriminelle var ute etter.

Ny trusselaktør som benytter utpressingsvare (ransomware/løsepengevirus)
Tre norske bedrifter ble offer for den relativt nye trusselaktøren Prometheus. De ble utsatt for datainnbrudd og en skadevare som krypterer alt innhold på nettverket, altså en type utpressingsvareangrep med såkalt dobbel utpressing. Dette er en aktør som gjennomfører sine angrep i løpet av veldig kort tid. Aktøren går inn og ut, ferdig kryptert på om lag 25 minutter. Første gang Prometheus slo til mot norske mål var i slutten av mai 2021. I de siste tilfellene har de utnyttet en sårbarhet i Fortigate-brannmurer, som gjør det mulig å hente ut brukernavn og passord fra tidligere SSLVPN-klienter i klartekst (CVE-2018-13379). Så fort de er på innsiden av VPN, starter de kartlegging av nettverket og identifisering av sårbare Windows-maskiner.

Bibliotek påvirket av dataangrep
Datasenteret til Axiell Norge (tidligere Bibliotekenes IT-senter) ble utsatt for et målrettet cyberangrep 22. juni. Tjenester de leverer til en rekke norske bibliotek og skoler ble utilgjengelige. Axiell leverer også tjenester til bibliotek i Sverige og Finland. Angrepet var av typen utpressingsvare og selskapet gjorde det tidlig klart at det ikke var aktuelt å betale løsepenger. Selskapet har meldt saken til politi i de respektive land. Axiell opplyste at ingen persondata skal være på avveie og at selskapet har backup av alle data.

Programvareleverandør Kaseya rammet av løsepengevirus
Den Florida-basert programvareleverandøren Kaseya ble 2. juni rammet av løsepengevirus. I en melding til sine kunder 5. juni, fortalte Kaseya at det var ca. 60 direkte-kunder og om lag 1500 kunder av kunder som hadde blitt rammet. Dette er kunder som kjørte en lokal versjon av selskapets VSA-produkt, en nettbasert plattform som brukes av store selskaper for å administrere arbeidsstasjoner og servere på eksterne steder. Aktøren REvil utnyttet en bug for å overta VSA-servere distribuert over hele verden og distribuere en kopi av REvil utpressingsvare til alle arbeidsstasjoner som var koblet til VSA-plattformen. I en melding som ble lagt ut på REvils portal på mørke nettet, hevdet trusselaktøren å ha infisert og kryptert filer på mer enn en million systemer under angrepet og krevde en løsepengesum på $70 millioner for å publisere en universell dekrypteringsnøkkel som kunne låse opp alle filer for alle Kaseya-kunder. En av virksomhetene som ble rammet av dette angrepet var Coop Sverige. Ikke alle butikkene i kjeden ble rammet, men pga. delvis havari på kassasystemet gikk Coop sin pressetalsperson ut og anmodet alle Coop-butikker om å holde stengt dagen etter angrepet.

Stort dataangrep mot norsk ingeniørselskap
Media kunne 7. juli fortelle at det norske ingeniørselskapet Inocean hadde vært utsatt for utpressingsvareangrep. Angrepet ble oppdaget en drøy uke tidligere. 2000 gigabyte med data skal ha blitt hentet ut av hackerne. Aktøren fulgte opp med å true Inocean med at de ville publisere materialet om selskapet ikke betalte utpressingskravet. Selskapet driver med skips-, offshore- og flytende vindkraftteknologi. I følge Inocean er det ikke snakk om sensitive data. Angriperne hevder de har lastet ned 10 prosent av dataene til selskapet. Det var hackergruppen REvil som skal stå bak angrepet.

GK-gruppen utsatt for dataangrep
GK-gruppen ble i juli angrepet av utpressingsvareangrep hvor interne systemer ble nedlåst. Angrepet ble oppdaget 17. juli. GK-gruppen, som er et skandinavisk entreprenørselskap med 3500 ansatte, sa til E24 at verken det operasjonelle eller kundedata var berørt. Selskapet har mange kommuner og offentlige virksomheter i Norge som kunder. GK-gruppen bekreftet til digi.no at det ble stjålet data fra serverne deres, og at de tar høyde for at personopplysninger er på avveie.

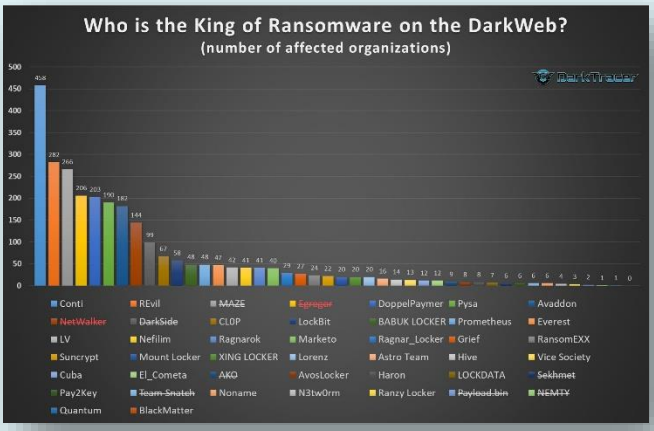
Accenture rammet av et utpressingsvareangrep.
Accenture ble 30 juli rammet av et cyberangrep med påfølgende kryptering og utpressing. Et internt notat ble angivelig sendt ut hvor de rapporterte at angriperne hadde stjålet både klientdata og arbeidsdokumenter. I midten av august publiserte LockBit Ransomware-as-a-Service (RaaS) -gruppen navnet og logoen til det som nå er bekreftet som et av deres siste ofre, altså Accenture. Accentures kunder inkluderer 91 av Fortune Global 100 og mer enn tre fjerdedeler av Fortune Global 500. I et innlegg på sitt nettsted på det mørke nettet tilbød LockBit Accenture-databaser for salg. Flere trusselaktører inkludert de som står bak LockBit, skriver nå at de rekrutterer aktivt bedrifters ansatte til å være innsidere for å hjelpe dem med å bryte og kryptere nettverk. Til gjengjeld blir innsideren lovet millionutbetalinger.

Situasjonsbilde og vurderinger:

Utpressingsvareangrep har blitt storpolitikk

Siden siste Situasjonsbilde publisert i april, har angrep, aktører og offersammensetning for utpressingsvareangrep/løsepengeangrep/ransomware utviklet seg via kjente trekk og trender. Noen aktører er nærmest forsvunnet (eks. Avaddon, REvil), andre har blitt tatt av politiet og nye har kommet til. Vi har tidligere nevnt at de kriminelle bak de avanserte utpressingsvare-angrepene er uformelt organisert, og danner verdikjeder hvor de forskjellige oppgavene utføres av ulike og ofte uavhengige grupper. En slik løs verdikjede gjør de kriminelle mindre sårbare for politiaksjoner fordi enkeltelementene i kjeden kan erstattes, og leddene vet ofte ikke nok om hverandre til å dra de andre med i dragsuget når noen blir tatt av politiet. Et slikt eksempel så man da ukrainsk politi (i samarbeid med USA og Sør-Korea) arresterte det mange trodde var banden bak Cl0p-utpressingsvaren. I stedet fanget de sannsynligvis bare pengevasker/kryptovaluta-delen av banden. Ytterligere indikasjoner på dette kom da Cl0p infiserte flere virksomheter etter tidspunktet for arrestasjonen. Cl0p-banden var tydeligvis fremdeles i full virksomhet.

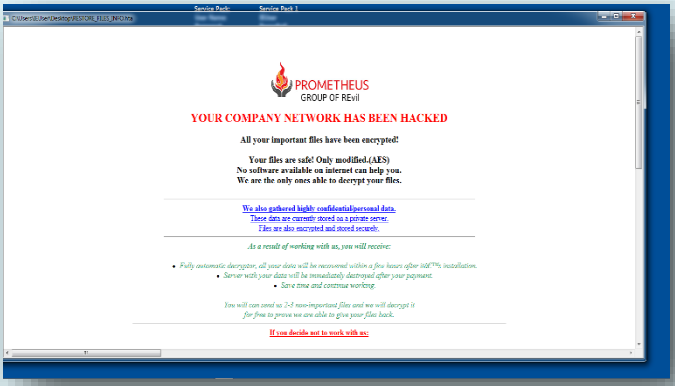
En annen trend er at vi oftere ser store selskaper og kjeder eller multinasjonale konsern bli rammet. Eksempler på dette er det nylige angrepet mot hundrevis av kunder av Kaseya-systemet (blant annet 800 svenske COOP-butikker), Colonial Pipepline rørledningen i USA og JBS - verdens største kjøttprodusent. Men også mindre, norske virksomheter og leverandører til det offentlige blir angrepet, blant annet Axiell biblioteksystem, Nordlo driftspartner i Haugesund, og Volue/Powel sine tekniske systemer er blitt rammet siden medio april 2021. Alle de tre nevnte leverer tjenester til norske kommuner, som i noen grad ble rammet av angrepene, da først og fremst i form av noe nedetid på tjenestene.



Figur 1: Ransomware-aktører som lekker på det mørke nettet (kilde: DarkTracer/Twitter)

USAs president Joe Biden har satt søkelys på bekjempelsen av denne formen for samfunnsnedbrytende kriminalitet. Det amerikanske justisdepartementet prioriterer nå for første gang etterforsking av slike angrep på linje med etterforskning av trusler mot nasjonal sikkerhet og terrorisme. I et møte med Putin 16. juni presset Biden på for å få russiske myndigheter til å bekjempe russiske kriminelle som står bak løsepengeangrep. I telefonsamtale med Putin 9. juli uttrykte Biden igjen utålmodighet med russiske myndigheters oppfølging av spor fra USA. Det antas at gruppen som står bak både Kaseya- og JBS-angrepene, og som går under navnet REvil, hører hjemme i Russland. Så skjer det snodige: REvil-banden som antas å stå bak de nevnte angrepene, forsvinner rett etter dette (13. juli) fra radaren, og deres lekkasje-web på det mørke nettet legges ned. Kaseya mottar et dekrypteringsverktøy fra en mystisk tredjepart som fungerer for alle rammede virksomheter som benytter Kaseyas systemer, og kundene kan gjenopprette systemene sine. Er verktøyet fra amerikansk etterretning, russisk etterretning, begge to i samarbeid, eller har Kaseya betalt REvil tilnærmet 70 mill USD som var kravet og fått verktøyet av dem? Kaseya hevder selv at de ikke betalte, men mottok en dekrypteringsnøkkel fra en "trusted third party". Primo september ser REvil ut til å være tilbake, og de har visstnok selv gått ut og hevdet at de har hatt «ferie» en stund. En logisk forklaring kan være at «noen» har vært på sporet av dem og at de har valgt å ligge lavt en periode.

Spekulasjonene er mange også rundt de andre forsvunnede aktørene, og hva det betyr: Er de tatt av politiet? Har russiske styresmakter og etterretning makt til å stoppe dem, og gjort det? Har de fått betalt og tatt seg en ferie? Er alle nykommerne egentlig en 'rebranding' av de som tilsynelatende har lagt ned virksomheten? Det er mye som tyder på at enkelte bander gjenoppstår i nye navn og ny forkledning. For eksempel antas det at gruppen Grief er rebranding av DoppelPaymer, Haron av Avaddon, BlackMatter av DarkSide og at LockBit 2.0 kommer fra REvil/Sodinokibi.



Figur 2 Prometheus Ransom Note (Kilde: Unit42/PaloAlto)

Noen løsepenge-bander har den siste tiden utvidet sine utpressingsmetoder; de presser nå kunder og partnere av ofrene for å legge ytterligere press på offeret. Angriper sender epost og informerer at data er stjålet fra offeret, og vil snart bli publisert på det mørke nettet hvis offeret ikke betaler. Hensikten kan både være å påføre offeret et indirekte press, eller faktisk bedrive utpressing direkte mot kunder eller partnere av offeret. Cl0p-banden og REvil er nevnt som eksempler på aktører som har begynt med denne taktikken, som også kalles kvadruppel utpressing (som en utvidelse av dobbel og trippel utpressing (DDos i tillegg). Det dukker stadig opp nye aktører (Prometheus Group of REvil, AvosLocker m.fl), og angrepene blir som nevnt mer avanserte, og raskere gjennomført enn noen gang. Guarden må heves heller enn å senkes.

Apropos utpressingsvareangrep: Etter Østre Toten-hendelsen har KPMG og kommunen nå i september publisert en interessant og lærerik rapport om sikkerhetstilstanden i kommunen forut for angrepet. Anbefales!

Business Email Compromise (BEC)

Business Email Compromise (BEC) er en type svindel som retter seg mot nær sagt alle typer virksomheter som gjennomfører bankoverføring. Bedrifts- eller offentlig tilgjengelige e-postkontoer til ledere eller nøkkelpersonell innen eksempelvis økonomi blir gjerne enten forfalsket eller kompromittert. Informasjonen eller kontoene blir så benyttet for å utføre eller få en person til å utføre en eller flere pengeoverføringer. En norsk oversettelse kan være: *Kompromittering av virksomhets-e-post*.

BEC er en av de største digitale truslene mot virksomheter i dag. Innenfor denne kategorien finner man eksempelvis direktørbedrageri, fakturasvindel, utpressings-epost, gavekortsvindel og andre typer emner som skal få deg til å utføre en oppgave for noen som svindlerne utgir seg for å være. Tilgang til en virksomhets e-post er spesielt verdifull for de kriminelle. Denne tilgangen kan de bruke både til å manipulere informasjon i en faktura, eller de kan kopiere og laste ned innhold som de senere bruker til utpressing. Et angrep starter ofte med en phishing-e-post der de kriminelle sikrer seg brukernavn og passord til en ansatt. Ved å lese e-post over lang tid, får bakmenn unik innsikt i virksomheten. Dette gir de kriminelle et godt grunnlag for å gjennomføre svindelen.

Det kan være ulike grunner til at akkurat din virksomhet blir valgt ut. Noen kriminelle jobber målrettet, mens andre jobber mer tilfeldig. Kanskje er det åpen informasjon på internett om virksomheten som gjør den interessant? Kanskje har de kriminelle tilgang inn i e-postsystemet til en virksomhet og leser all

korrespondansen virksomheten har med kundene fordi en ansatt har vært utsatt for phishing. Eller det kan være at passord og brukernavn til en brukerkonto ligger tilgjengelig på det mørke nettet.

Metodene de kriminelle benytter for lykkes med denne typen svindel varierer. Kriminelle kan forfalske e-postadresser til å ligne på adresser tilknyttet en virksomhet, de kan bruke phishing eller allerede tilgjengelige brukernavn og passord for å skaffe seg tilgang til en e-postkonto, eller de kan sende en programvare som installeres på e-postserveren slik at de får tilgang til all e-post hos virksomheten. Med denne tilgangen kan de lære seg hvordan prosesser i virksomheter fungerer, forstå språk og ikke minst detaljer som signaturer mm. Deretter bruker de mulighetene de har opparbeidet seg, gjerne sammen med sosial manipulasjon til å få overført penger til en konto de selv kontrollerer. Enkelte kriminelle grupper har spesialisert seg på forskjellig bransjer slik at de kjenner faguttrykk og andre faktorer typisk for bransjen. På denne måten kan de skape stor grad av troverdighet i sine angrep.

K-CSIRT har det siste året spesielt fulgt med på noen kampanjer. Dette har hovedsakelig vært tilfeller hvor de kriminelle har forsøkt å lure/stjele til seg passord fra offeret ved hjelp av phishing-e-post. Mange ulike merkevarer misbrukes i phishing-kampanjer, og vi har sett phishing mot virksomheter hvor det har blitt brukt forfalskede e-poster som gir seg ut for å være fra Microsoft og gjerne oppgradering av Office 365-konto, eller et tema tilknyttet helpdesk og utfordringer med Teams-lenker. I e-poster fra svindlere, knyttet til BEC-svindel med spoofede (norsk: etterlignede/imiterte) e-postadresser, benyttes ofte ord og emner som forespørsel, betaling, overføring og presserende, blant andre.

Når de kriminelle har stjålet brukernavn og passord har de tilgang til å lese all e-post på denne kontoen. De kan sende og slette e-post og de kan sette opp faste regler - for eksempel kan de videresende all e-post til en konto de selv kontrollerer. To-trinns autentisering og One Time Password (OTP) vil komplisere et slikt angrep. Selv om det finnes veier rundt, kan dette føre til at de kriminelle ikke får tilgang til e-post eller at de velger et mål som er enklere å kompromittere. K-CSIRT har også tidligere sett at e-poster kan fremstå som å komme fra en pålitelig leverandør/kunde av en virksomhet som dermed kan være offer for spoofing eller reelt har en eller flere kompromitterte kontoer. Dette er svært utfordrende for virksomheten som mottar e-posten siden de allerede har et kunde/leverandør forhold til «avsender».

FBI blant andre har spesielt trukket frem fem typer BEC-svindel:

- Bedrifter med utenlandske leverandører er ofte mål med taktikken der angripere later til å være leverandørene som ber om pengeoverføringer for betaling til en konto som eies av svindlere.
- Kriminelle utgir seg som selskapets administrerende direktør eller en leder og sender en e-post til ansatte på økonomiavdelingen og ber dem om å overføre penger til kontoen de kontrollerer.
- Kontoovertakelse - En leder eller ansattes e-postkonto blir hacket og brukt til å be om fakturabehandling til leverandører oppført i e-postkontaktene. Betalinger blir deretter sendt til angripers bankkonto i stedet for til leverandørens.
- Advokatimitasjon - Angripere later til å være advokat eller noen fra advokatfirmaet som angivelig har ansvaret for viktige og konfidensielle forhold. Normalt gjøres slike falske forespørsler via e-post eller telefon, og i løpet av arbeidsdagen.
- Datatyveri – HR- og økonomiansatte er mål for svindel hvor kriminelle forsøker å skaffe personlig identifiserbar informasjon til ansatte og ledere. Slike data kan brukes til fremtidige angrep. Her har man sett e-poster hvor kriminelle utgir seg for å være en ansatt som ønsker å bytte kontonummer for å få lønn inn på en ny konto.

Figur 3 Mange navn - én forbrytelse (Kilde: Interpol)

BEC-angrep er ofte veldig skjult, med angripere som gjemmer seg ved å blande seg i legitim trafikk ved hjelp av IP-områder med høyt omdømme og ved å utføre diskrete aktiviteter på bestemte tidspunkter og innen spesielle forbindelser. BEC-angrep kan dessverre forbli uoppdaget til de forårsaker reelt store økonomiske tap. Dette på grunn av begrenset eller delvis synlighet fra sikkerhetsløsninger som ikke drar nytte av omfattende synlighet i e-posttrafikk, identiteter, endepunkter og skyadferd, samt muligheten til å kombinere sammen isolerte hendelser, og levere en mer sofistikert tilnærming på tvers av domener.

Hva kan du og din virksomhet gjøre for og reduserer risikoen for å bli svindlet?

- Tofaktor-autentisering for innlogging på bedriftens systemer og transaksjoner.
- Lære opp ansatte med spesielle rettigheter til å være mistenksomme.
- Bedrifter bør ha kommunikasjonsrutiner for å minske risikoen for at denne typen svindel inntreffer.
- Regelmessig gjennomgang av sikkerhetsrutiner og policy.
- Følge «least privilege»-prinsippet som handler om å gi ansatte færrest mulige tilganger.
- Rapporter alltid dersom du tror noe er svindel.
- Ta i bruk SPF/DKIM/DMARC for epost. Dette forsikrer at avsender er verifisert.

Konklusjon

Opplæring av ansatte i å kjenne igjen tegn til phishing og implementering av organisatoriske tiltak og rutiner er en god investering. Dog er det også viktig å investere i teknologi og annen støtte som kan oppdage og varsle brukerne om truslene kontinuerlig, kombinert med teknologi som automatisk isolerer maskinen, låser brukeren eller på annen måte forhindrer angriperen i å lykkes. Men kan i tillegg bruke et slikt verktøy til å aktivt lære ansatte riktig bruk av data, holde de oppdatert på lover, regler og rutiner samtidig som man aktivt forhindrer de å bryte disse. K-CSIRT tror på et godt samarbeid mellom ansatte, prosesser og teknologi.

Kilder

- https://www.politiet.no/globalassets/dokumenter/oslo/naringslivskontakten---forebyggende/virksomhetsbedrageri.pdf
- https://www.ic3.gov/Media/News/2021/210318.pdf
- https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-email-security/business-email-compromise-bec/

Glasskula – hva ser vi komme?

Digitale angrep mot norske virksomheter vil fortsette som før. Norske kommuner og fylkeskommuner er i endring, både mot mer digitalisering og mer skytjenester. Dette skaper flere sårbare grenseflater og dermed økte muligheter for vellykkede angrep fra de som ønsker å utnytte dette.

Mest alvorlige trussel fremover: Avansert løsepengeangrep med dobbel utpressing.
Denne virksomheten har blitt så alvorlig at President Biden har advart Russland mot å være vertskap for disse bandene uten å stoppe dem. Økt oppmerksomhet og storpolitiske agendaer kan selvsagt bidra til å stoppe noen aktører, men den kriminelle strukturen virker så fleksibel, profesjonell og fragmentert at disse tiltakene ikke reduserer trusselen mot norske kommuner i nevneverdig grad.

Svindel ved hjelp av BEC
Ulike typer svindelkampanjer ved hjelp av e-post er svært vanlige, og vil også i tiden fremover dominere bildet av farlige kampanjer mot norske virksomheter. Kompromitterte kontoer er av stor verdi for kriminelle, og kan benyttes til flere svindelformål.

Andre trusler
Økt netthandel grunnet pandemien har medført en myriade av forskjellig phishing-kampanjer. Særlig aktive har de kriminelle vært på SMS, hvor store firma har vært spoofet gjennom en kampanje som kalles FluBot. Mottager blir for eksempel bedt om å laste ned DHL-appen fra en lenke i SMS, men det man laster ned er en skadelig app som både lekker data om deg og kan medføre banksvindel.

På sensommeren er det observert kampanjer som benytter hackede Facebook-kontoer til å lure ofre til å sende verifiseringskoder for passordbytte til dem ved å hevde at de er påmeldt en konkurranse eller lignende. Vi vurderer det som sannsynlig at det blir en økning av mer sofistikert 'smishing' samt bruk av chattetjenester i tiden fremover for å tilegne seg påloggingsdetaljer.

Vi vurderer det slik at Covid-19 relaterte tema vil fortsette å være synlige i kampanjer, og at nye tema for denne typen kampanjer kan omhandle klimakrisen og tiltak for reduserte karbonutslipp.

Rapporten «IT i Praksis 2021» ble lansert den 2. september. Det er uttalt tidligere at IT i praksis er et verdifullt redskap for statlige og kommunale virksomhetsansvarlige og digitaliseringsansvarlige i deres arbeid med å nå målene for digitalisering frem mot 2025. I FNs klimapanels nylig fremlagte rapport går det tydelig frem at det haster med å finne løsninger på klimakrisen. Digitale løsninger vil spille en sentral og avgjørende rolle for at vi skal nå utslippsmålene. IT i Praksis viser at bare 37% av respondentene oppgir at de har tilstrekkelig kompetanse på informasjonssikkerhet. En av aktørene som står bak undersøkelsen er IKT-Norge. IKT- Norge er etter å ha vært gjennom svarene i undersøkelsen svært bekymret for hva som vil skje dersom teknologiens inntog i offentlig sektor ikke også kommer med strengere krav til digital sikkerhet og personvern.

Det bedrives svært mye godt sikkerhetsarbeid i kommunal sektor og mange kommuner har god kompetanse på området, men vi deler IKT-Norge sin bekymring - særlig når vi må lete etter sikkerhetsdesign i digitaliseringsprosjekter. Sikkerhetsdesign må etter vår mening være en parallell prosess i all digitalisering.

Siste side

Rapportens aktuelle situasjonstips:

For brukere:

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

For driftspersonell:

- Sørg for to-faktorautentisering for *all* tilgang utenfra
- Ikke la utrangert utstyr bli stående eksponert mot internett
- Oppgrader alt internett-eksponert utstyr så raskt det lar seg gjøre - angrepene mot disse øker
- Gjennomfør andre tiltak som hindrer løsepengeangrep (se rapport, varsel fra NSM, DSB og K-CSIRT - https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/varsler-fra-ncsc/varsel-om-losepengevirus eller ta kontakt med oss)
- Sørg for å ha sikkerhetskopier som er reelt offline

Relevante rapporter, dokumenter og kampanjer lansert i perioden:

Rapport fra KPMG: IKT-sikkerheten i Østre Toten Kommune forut for dataangrepet 9. januar 2021.
https://www.ototen.no/aktuelt/ikt-sikkerheten-for-angrepet-kartlagt-og-vurdert.13134.aspx

NSM, DigDir og DFØ: Ny veileder gir råd om helhetlig styring av informasjonssikkerhet
https://nsm.no/aktuelt/ny-veileder-gir-rad-om-helhetlig-styring-av-informasjonssikkerhet

Ramboll m-fl: «IT i praksis» er en omfattende og viktig undersøkelse om strategisk og forretningsmessig bruk av IT i både private og offentlige virksomheter
https://no.ramboll.com/presse/publikasjoner/it-i-praksis-2021

Gjør deg kjent med Nasjonal sikkerhetsmåned 2021 – Kampanjen koordineres nasjonalt av NorSIS. Les mer om kampanjen på: https://sikkert.no/

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.**