WATCHCOM
A COMBITECH COMPANY

RANSOMWARE

WHITEPAPER V2.0 – 14.06.2022

Forfatter: Frank Haugnes, Senior Information Security Specialist

INNHOLDSFORTEGNELSE

INTRODUKSJON

I løpet av 2021 har det vært en markant økning i antallet ransomware-angrep. Iht. "2022 SonicWall Cyber Threat Report" har det for Europa vært en økning på 175% i observerte ransomware-angrep i løpet av 2021. Iht. en undersøkelse fra NRK har ransomware rammet minst 24 norske virksomheter og kostet nærmere én milliard kroner. Dette er kun snakk om offentlig kjente hendelser. Det er sannsynligvis snakk om langt høyere summer, ettersom det er vanskelig å beregne de totale kostnadene ved et dataangrep og at mange dataangrep heller aldri blir kjent for offentligheten.

HVA ER RANSOMWARE?

"Skadevare" er samlebetegnelse på skadelig programvare som - hvis den kjøres - kan forårsake skade på brukerens systemer eller informasjon. Eksempler på slik skade er:

- Enheter blir låst eller ubrukelige.
- Data blir stjålet, slettet eller kryptert.
- Det blir tatt kontroll over enheter for å bruke disse i angrep på andre virksomheter.
- Tyveri av brukeridentifikasjoner som gir tilgang til virksomhetens systemer eller tjenester.
- Det blir tatt kontroll over enheter for å bruke disse til andre formål, eks. utvinning av kryptovaluta.
- Bruk av tjenester som kan koste deg penger (f.eks. telefonsamtaler med høy pris).

Ransomware (også kalt "løsepengevirus", "krypteringsvirus", "utpressingsvare", "utpressingsprogramvare" eller "gisselvare") er en type skadevare som forhindrer eller begrenser offeret fra å få tilgang til enheten sin, enten ved å låse maskinen eller ved å kryptere filer på maskinen. De fleste løsepengevirus krypterer innholdet på slik måte at det er svært vanskelig å låse opp filene uten tilgang til dekrypteringsnøkkelen. Angriperen krever løsepenger fra offeret for dekrypteringsnøkkelen som gjenoppretter tilgangen til dataene. Kostnadene kan variere fra noen hundre dollar til tusenvis, vanligvis utbetalt i kryptovaluta (f.eks. Bitcoin).

Det er en økende trend at angripere også truer med å publisere sensitiv data dersom du ikke betaler (dobbel utpressing). Selv om du betaler, kan angriperen likevel publisere eller selge dataene. Det er derfor viktig at virksomheten iverksetter tiltak for å minimere virkningen av dataeksfiltrering (kopiering og tyveri av data). I tillegg er det enkelte ransomware-aktører som truer med å gjennomføre DDoS-angrep (tjenestenekt-angrep) hvis betaling uteblir (trippel utpressing).

> "***Det er en svært høy risiko for at flere norske virksomheter vil utsettes for løsepengevirus i løpet av 2022. Det er også mulig at norske virksomheter vil utsettes for løsepengevirus med omfattende konsekvenser.***" NSM, Nasjonalt digitalt risikobilde 2021

Ransomware er på ingen måte et nytt fenomen. Allerede i 1998 ble ideen om ransomware konseptualisert med den såkalte "AIDS Trojan". Denne ble distribuert på en diskett som ble

sendt i posten til ofrene. Etter dette var det ganske lite utvikling på ransomware-fronten fram til Cryptolocker kom i 2013. Cryptolocker brukte kryptering med AES-256 for å kryptere filer, og krevde betaling i den nye valutaen Bitcoin, noe som gjorde det mye vanskeligere å spore de kriminelle som sto bak. Dette åpnet for en helt ny, stor, økonomi rundt utpressing med ransomware, og i dag har vi et sort antall varianter av disse. I løpet av 2021 observerte forskere fra SonicWall Capture Labs omtrent 1000 unike ransomware-signaturer og over 300 ransomware-familier. En analyse utført av forskere ved Chainalysis tyder på at 74 % av alle pengene som ble tjent gjennom ransomware-angrep i 2021, over 400 millioner dollar i kryptovaluta, gikk til Russland-tilknyttede "hackere".

Infeksjoner av ransomware i datautstyr skyldes typisk skadevare spredt med e-post. Iht. NorSIS sin rapport "Trusler og trender 2019-2020" er andelen norske bedrifter som har vært angrepet eller forsøkt angrepet med ondsinnede e-poster på 56%, og det har vært en markant økning i svindel-e-post ifm. Covid-19-pandemien.

Den mest kjente ransomware-hendelsen i nyere tid var cyberangrepet på Hydro i mars 2019. Hydro har estimert den totale kostnaden av cyberangrepet til rundt 800 MNOK.

"Politiets Trusselvurdering 2021" sier om ransomware at "*Globalt er det anslagsvis 5–15 internasjonale aktører som er aktive til enhver tid. I Norge har vi informasjon om at én aktør alene har gjennomført over 30 vellykkede datainnbrudd mot norske bedrifter det siste året.*"

HVORDAN VIRKER RANSOMWARE?

Når ransomware har infisert en maskin kan enten skjermen låses, eller, i tilfellet krypto-ransomware, forhåndsbestemte filtyper krypteres. I det første scenariet vises et fullskjermbilde eller et varsel på den infiserte maskinens skjerm, noe som forhindrer ofrene i å bruke maskinen. Skjermbildet viser også instruksjoner til hvordan offeret skal betale løsepengene. I det andre scenariet forhindres tilgang til filer med potensielt kritisk eller verdifullt innhold ved å kryptere bestemte filtyper som .DOCX, .XLSX, .PDF, .JPG, .ZIP og andre vanlig brukte filtyper. Ransomware legger vanligvis til en egen fil-utvidelse på filnavnet til de krypterte filene, som f.eks. .aaa, .micro, .encrypted, .ttt, .xyz, .zzz, .locky, .crypt, .cryptolocker, .vault, eller .petya, for å vise at filene er kryptert - filtypen som brukes er vanligvis unik for den enkelte ransomware-typen.

Fig. 1 – Eksempel på varsel på den infiserte maskinens skjerm

HVORDAN DISTRIBUERES RANSOMWARE?

En av de vanligste angrepsvektorene er phishing-e-post - et vedlegg (eller en hyperlink) som kommer til offeret i en e-post, og som kamufleres som en fil (eller hyperlink og kilde) de kan stole på. Straks linken er klikket på, eller vedlegget er lastet ned og åpnet, kan de ta over offerets datamaskin, spesielt hvis skadevaren har innebygde verktøy som lurer offeret til å gi administrativ tilgang (social engineering tools). Andre mer aggressive former for ransomware, som f.eks. NotPetya, utnytter sikkerhetshull for å infisere datamaskiner uten å lure brukere. Ransomware kan også lastes ned på systemer når brukere besøker ondsinnede eller kompromitterte nettsteder (Drive-by Compromise).

I korte trekk følger ransomware-angrep prosessen i figuren nedenfor.

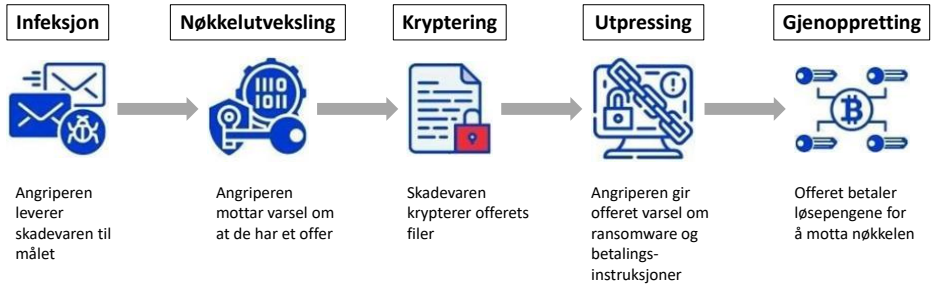

Fig. 2 – Angrepsprosessen for ransomware

De vanligste måtene for distribusjon av ransomware er:

- **Phishing** – en type angrep som bruker tekst, e-post eller sosiale medier for å lure brukere til å klikke på en ondsinnet lenke eller et vedlegg. Phishing-forsøk er ofte generelle masseutsendelser, men meldingen ser ut til å være legitim og fra en pålitelig kilde (f.eks. en bank). Ondsinnet kode vil eksekvere kommandoer ved å bruke tilgangsrettighetene dine. Angriperen kan også bruke denne muligheten til å installere en "bakdør" på enhetene dine.
- **Drive-by downloads** - skjer når en bruker ubevisst besøker et infisert nettsted der skadelig programvare lastes ned og installeres uten brukerens viten.
- **Malvertising** - ondsinnet kode er injisert i legitime nettannonser. Når en bruker klikker på annonsen, blir skadelig programvare lastet ned og installert uten brukerens viten.
- **Eksponerte tjenester** – nettverksinntrenging gjennom dårlig sikrede porter og tjenester, eksempelvis Remote Desktop Protocol (RDP), som gir tilgang til enhetene dine. Angriperen kan bruke en rekke taktikker, som å utnytte vanlige sårbarheter og "passordspraying", for å få tilgang til enhetene dine via disse utsatte systemene og distribuere ransomware.

Selv om de følgende elementene ikke er definert som angrepsvektorer, er de gode tilgjengelige alternativer for angripere å bruke for å sette i gang et ransomware-angrep:

- **Identiteter for tredjeparter og administrerte tjenesteleverandører (MSP)** - kan brukes av angriper til å forfalske e-poster eller utføre phishing-angrep mot virksomheten.
- **Leverandørkjede-angrep** – dårlig sikret programvare, it-systemer eller tjenester hos en leverandør kan angripes, og angriperen benytter tilgangen til disse som springbrett for å bryte seg inn i kundenes it-systemer. Angriperen kan også skjule skadevare med "bakdører" i produkter som leverandøren selger til sine kunder, og skadevaren kan bli med i en programvare-oppdatering. Angriperen utnytter tillitsforholdet mellom leverandør og kunde, hvor kundene ukritisk installerer en kompromittert programvare eller oppdatering i den tro at denne er legitim. Angriperen kan dermed utnytte bakdøren for videre kompromittering av kundene. Eksempler på dette er Windows Update og SolarWinds-hendelsene.
- **Ransomware as a Service (RaaS)** - en tjenestemodell der angripere, uavhengig av deres ferdigheter, kan kjøpe skadevare fra utviklere på det mørke nettet. Utviklerne mottar en del av løsepengene betalt av offeret.

OFTE BRUKTE TAKTIKKER OG TEKNIKKER

Rammeverket MITRE ATT&CK ble opprettet av MITRE i 2013 som et verktøy for å dokumentere angrepstaktikker og -teknikker basert på virkelige observasjoner. Dette rammeverket har med tiden blitt en velkjent kunnskapsbase for sikkerhetsbransjen for å forstå angrepsmodeller, metoder og mottiltak. Rammeverket utvikles fortløpende med endringene i trussellandskapet.

Idéen bak rammeverket er at alle cyber-angrep følger gitte faser:

Fig. 3 – MITRE ATT&CK

Rammeverket definerer hvilke teknikker angriperen benytter i hver fase, og denne informasjonen brukes som grunnlag for utvikling av spesifikke trusselmodeller og metoder. Målet med rammeverket er å bedre kunne detektere angrep eller kompromittering ved å illustrere hvilke aktiviteter en angriper kan ha gjennomført:

- Hvordan kom angriperen seg inn?
- Hvordan beveger de seg rundt i IT-systemene?

Ved å gi svar på slike spørsmål kan rammeverket brukes til å identifisere huller i forsvaret, og prioritere dem basert på risiko.

MITRE ATT&CK-matrisen i Vedlegg 1 viser taktikker og teknikker som vanligvis benyttes ved ransomware-angrep. Disse er oppført fra de vanligste (røde) til de mindre vanlige (gule), og er angitt med deres respektive ATT&CK-ID. Disse ID-ene finnes på MITRE ATT&CK-nettstedet

sammen med ytterligere detaljer om individuelle TTP-er (tactics, techniques and procedures) og potensielle mottiltak.

I matrisen er teknikker angitt for alle faser fra initiell tilgang og fram til at angriperens mål er nådd. Teknikker for fasene "Reconnaissance" og "Resource Development" er ikke angitt da disse primært dreier seg om forarbeidet angriperen gjør for å forberede et angrep og bygge opp ressursene sine.

HVEM ER TRUSSELAKTØRENE BAK RANSOMWARE?

Generelt er det følgende kategorier av trusselaktører som opererer via internett:

- Sofistikerte statsstøttede trusselaktører
- Profesjonelle, organiserte kriminelle
- Cyberterrorister
- Politisk/ideologisk motiverte grupper (Hacktivistgrupper)
- Politisk/ideologisk motiverte enkeltpersoner (Hacktivister)
- Script Kiddies

Det er ofte kriminelle syndikater som står bak forsyningskjeder for "cybercrime services for sale". Disse tjenestene fortsetter å modnes, og "alle" kan kjøpe de tjenestene som trengs for å utføre ondsinnet aktivitet for økonomisk vinning eller andre ondsinnede formål.

Figuren nedenfor viser gjennomsnittlig prisnivået for slike tjenester:

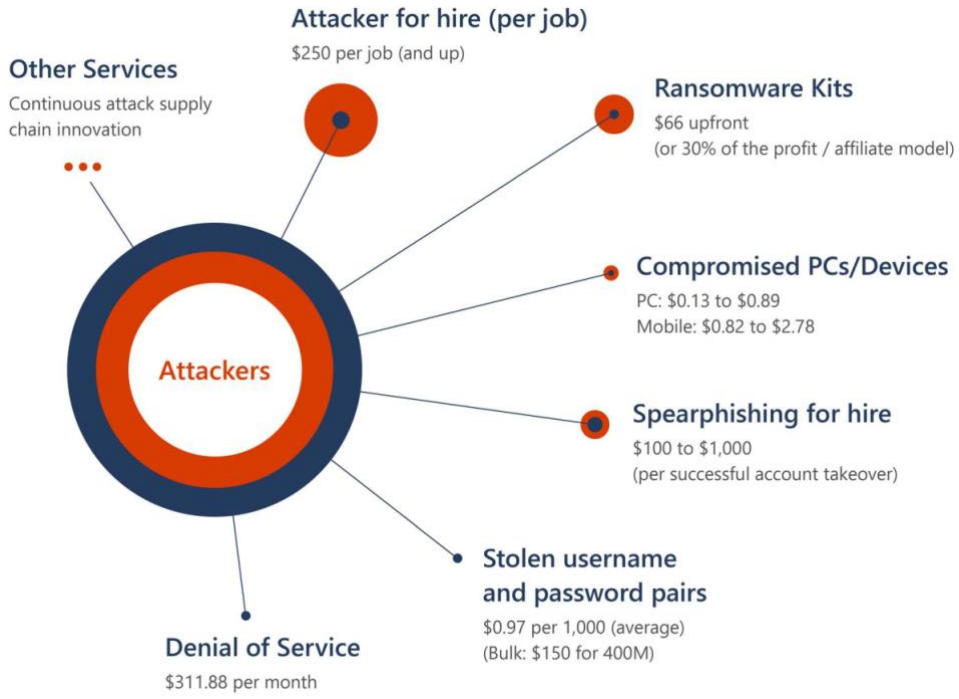

Fig. 4 – Gjennomsnittlig prisnivå for "cybercrime services for sale"
Kilde: Microsoft Digital Defense Report - October 2021

Hovedsakelig benytter følgende grupper av trusselaktører ransomware som verktøy for å oppnå sine mål:

Økonomisk motiverte trusselaktører: Profitt er en av de vanligste motivasjonene til trusselaktører. Nettkriminalitet anses som en gullgruve for kriminelle, og angriperne trenger ikke å være sofistikerte for å utføre disse forbrytelsene. De er opportunistiske og sikter mot "lavthengende frukter". Trusselaktørene er ikke opptatt av om angrepene deres blir oppdaget fordi de kun er interessert i å erverve seg data og informasjon som kan omsettes til penger så raskt som mulig. Det er både organiserte ransomware-bander og uavhengige kriminelle som kjøper ransomware gjennom Ransomware-as-a-Service-operatører.

Det er også kjente tilfeller der sofistikerte statsstøttede trusselaktører har blitt benyttet for å gi inntekter til staten, f.eks. Nord-Korea og Iran. Felles for disse landene er at de har reduserte inntekter på grunn av internasjonale sanksjoner, og dermed tyr til kriminell aktivitet for å øke sine inntekter.

Politisk og ideologisk motiverte trusselaktører: Hacktivisme defineres som individer eller grupper som bruker "hacking" for å påvirke politiske eller sosiale endringer. Det hacktivistiske landskapet er mangfoldig, og omfatter en rekke individer og grupper på ulike nivåer av ferdigheter og evner. Hacktivister er kjent for å bruke skadelig programvare, DDoS-angrep, "doxing", defacing av nettsider og sosiale medier for å avsløre inkriminerende informasjon om målet deres; alt fra "urettferdig" forretningspraksis til hemmelighold av myndighetene. Den mest kjente activist/hacktivist-gruppen er Anonymous.

Et eksempel på et politisk motivert angrep er der en hviterussisk hackergruppe hacket seg inn i datanettverkene tilknyttet jernbanen som frakter russisk utstyr inn i landet.

NSM regner også med at de samme metodene som benyttes med skadevare også benyttes i forbindelse med spionasje, uten at det kommer krav om løsepenger. Slik spionasje kan være rettet mot norsk industri og mot norske myndigheter. Denne typen angrep kan potensielt pågå uoppdaget i årevis, og være skadelig for både virksomheten og nasjonens sikkerhet. De samme tiltakene som hjelper mot ransomware beskytter også mot skadevare som har spionasje som formål.

HVEM ER MÅLGRUPPER FOR RANSOMWARE-ANGREP?

Ransomware retter seg mot hjemmebrukere, bedrifter og offentlige nettverk. Det kan føre til midlertidig eller permanent tap av sensitiv eller proprietær informasjon, forstyrrelser av vanlige aktiviteter og drift samt redusert produksjonsevne. Det vil også medføre økonomiske tap for å gjenopprette systemer og filer, og omdømmeskade for organisasjoner. Hele samfunnet blir berørt når kritiske samfunnsfunksjoner blir satt ut av spill.

Mens alle bransjer er mulige mål for ransomware-angrep, er noen mere berørt enn andre. Dette inkluderer detaljhandel, juss/finans, produksjon og jordbruk/matproduksjon, myndigheter, helsevesen og utdanning. Figuren nedenfor viser hvordan ransomware-angrep fordeler seg blant de forskjellige bransjene:

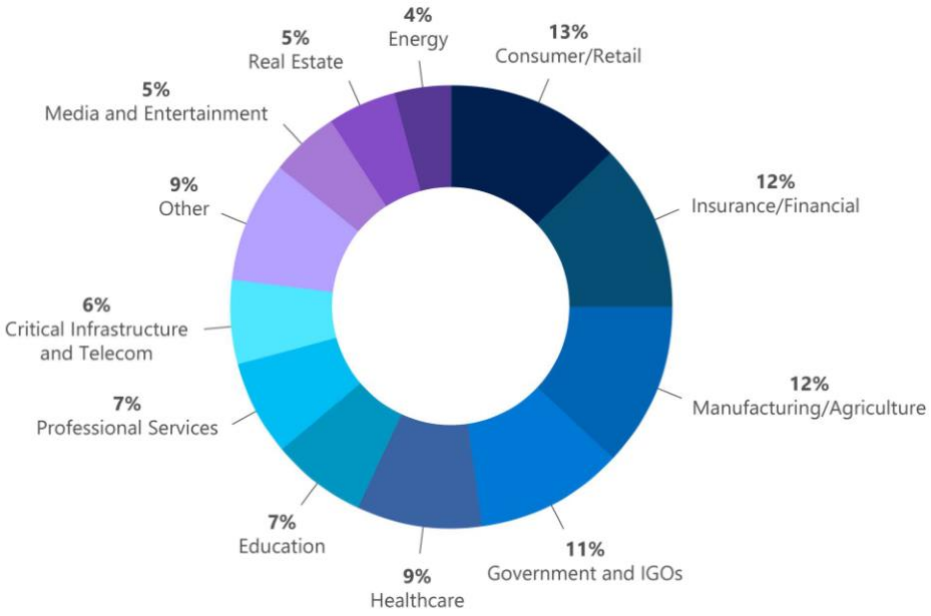

Fig. 5 – Fordelingen av ransomware-angrep per bransje (Juli 2020-Juni 2021)
Kilde: Microsoft Digital Defense Report - October 2021

De organiserte gruppene er ofte mer målrettet i valg av ofre, mens opportunistene satser på tilfeldige mål. Organiserte grupper angriper kritisk infrastruktur, større selskaper, offentlig sektor (helse, utdanning, kommuner, byer etc.) da disse sannsynligvis har økonomisk kapasitet til å betale løsepengene. Opportunistene satser på å ramme flest mulig med sine angrep, og satser på at i hvert fall noen av ofrene har mulighet til å betale.

Et godt eksempel på et målrettet angrep er den mye omtalte "Colonial Pipeline ransomware attack" hvor den russisk-baserte DarkSide-gruppen angrep, og satt ut av drift, Colonial Pipeline, det største rørsystemet for transport av raffinerte oljeprodukter i USA.

SKAL DU BETALE LØSEPENGENE?

Ikke betal kriminelle: Beslutningen om å betale en trusselsaktør for å tilgang til filene eller enhetene dine er vanskelig, og du kan føle deg presset til å gi etter for trusselaktørens krav. Uansett trussel eller krav anbefaler vi at det første du gjør er å rapportere hendelsen til politiet. Videre støtter vi oss til NSMs generelle råd om ikke å betale løsepenger. Dette blant annet på grunn av følgende:

- Å betale løsepengene gir ingen garanti for at du får tilgang til filene eller enhetene dine. Trusselaktører kan kreve mer penger til tross for at de har mottatt den første utbetalingen.
- Å betale oppfordrer trusselaktører til å fortsette å angripe enhetene dine da de regner med at du også vil betale ved neste angrep.
- Trusselaktører kan bruke "wiper-malware" som utgir seg for å være ransomware. I dette tilfellet kan ikke filene dine gjenopprettes ettersom skadevaren gjør uopprettelig skade på dem når løsepengene er betalt.

- Dataene dine har sannsynligvis blitt kopiert og kan lekkes av trusselaktøren. De kan også fortsette utpressingen med de kopierte dataene.
- Betalingen din kan bli brukt til å støtte annen kriminell virksomhet eller terrororganisasjoner.

Hvis du blir utsatt for et ransomware-angrep og ikke har sikkerhetskopi av alle filene, kan det i noen tilfeller finnes verktøy for dekryptering av låste filer. Gå inn på nomoreransom.org og sjekk om det finnes et dekrypteringsverktøy for den typen ransomware du er rammet av. Hvis du ikke får dekryptert filene selv anbefales det å kontakte en spesialist på gjenoppretting av data.

HVORDAN BESKYTTE SEG MOT RANSOMWARE

Det er en del tiltak du kan gjøre for å forberede virksomheten din mot potensielt skadelig programvare og ransomware-angrep. Vurder beste praksis og tiltakene nedenfor for å håndtere risikoen fra ransomware og støtte virksomheten i å koordinere og effektivisere respons på en ransomware-hendelse. Implementer tiltakene i størst mulig grad basert på virksomhetens muligheter og ressurser.

Tiltakene adresserer grovt sett disse sikkerhetsmålene:

- Forhindre at skadevare infiserer enheter og sprer seg.
- Forhindre at skadevare eksekverer på enheter.
- Redusere konsekvensene av skadevare.
- Forbered virksomheten på en hendelse.

I tillegg er det tiltak som du kan iverksette øyeblikkelig dersom virksomheten er utsatt for en ransomware-hendelse.

SIKKERHETSPLANLEGGING

Informasjonssikkerhet dreier seg om å håndtere risiko relatert til virksomhetens informasjonsverdier, og omfatter bl.a.:

- **Konfidensialitet** – at informasjonen ikke blir kjent for uvedkommende.
- **Integritet** – at informasjonen ikke blir endret utilsiktet eller av uvedkommende.
- **Tilgjengelighet** – at informasjonen er tilgjengelig for autoriserte ved behov.
- **Robusthet** – at organisasjonen og systemene er motstandsdyktige, og evner å gjenopprette normaltilstand ved hendelser.

Informasjonssikkerhet oppnås ved hjelp av både tekniske og organisatoriske tiltak, og effektiv informasjonssikkerhet fordrer en god sikkerhetsplan som bør holdes oppdatert til enhver tid.

Bruke en "forsvar i dybden"-strategi

Siden det ikke er noen måte å fullstendig beskytte seg mot skadelig programvare, bør du følge en "forsvar i dybden"-strategi. Dette innebærer lagvis beskyttelse med flere

sikkerhetstiltak i hvert lag. Slik vil du ha flere muligheter til å oppdage skadelig programvare, og deretter stoppe den før den forårsaker reell skade for virksomheten. Du bør anta at skadelig programvare kommer til å infiltrere virksomheten, og du bør derfor ta nødvendige skritt for å begrense effekten dette vil føre til, og øke responsevnen.

NSMs Grunnprinsipper for IKT-sikkerhet definerer et sett med prinsipper og underliggende tiltak for å beskytte informasjonssystemer (maskinvare, programvare og tilknyttet infrastruktur), data, og tjenestene de tilbyr mot uautorisert tilgang, skade eller misbruk. Prinsippene skal bidra til å heve sikkerhetskompetanse og sikkerhetsnivået i norske virksomheter og er relevante for alle virksomheter, både i offentlig og privat sektor. Vi oppfordrer spesielt virksomheter som er ansvarlige for samfunnskritiske funksjoner til å benytte seg av prinsippene og følge dem i så stor grad som mulig.

Gi personalet ditt opplæring

Angripere kommer seg ofte inn i en virksomhet ved å lure en bruker til å avsløre et passord eller klikke på virusinfiserte e-postvedlegg eller linker.

Vi anbefaler at det etablers et program for sikkerhetsopplæring og bevisstgjøring av de ansatte som inkluderer veiledning om hvordan man identifiserer og rapporterer mistenkelig aktivitet (f.eks. phishing) eller hendelser.

Alle ansatte bør være bevisste på at ransomware lett kan treffe dem via en phishing-e-post, tvilsomme nettsteder, eller "cracked" programvare lastet ned fra uoffisielle kilder.

Vi anbefaler også at virksomheten

- Sørger for at personalet til enhver tid er årvåkne, og påminner brukerne om å aldri klikke på uønskede lenker eller åpne uønskede vedlegg i e-post.
- Gjennomfører kontinuerlige phishing-tester i hele virksomheten for å måle sikkerhetsbevisstheten og forsterke viktigheten av å identifisere potensielt ondsinnede e-poster.

TILTAK MOT SKADEVARE OG DIGITAL UTPRESSING

NSM har publisert en samleside for "Digital utpressing (løsepengeangrep)" der du også finner en oversikt over NSMs tiltak mot skadevare og digital utpressing (løsepengeangrep). Nedenfor er tiltakene oppsummert. Detaljer for hvert av disse tiltakene er å finne i "Regnearket med sikkerhetstiltak" fra NSM.

Planlegg for å hindre (redusere konsekvens) og håndtere dataangrep med skadevare:

1. Ha en plan for teknologiske tiltak.
2. Ha en plan for sikkerhetskultur.
3. Identifiser virksomhetens viktigste verdier og tjenester.
4. Forbered virksomheten på et dataangrep.
5. Ta på forhånd stilling til juridiske, økonomiske, sikkerhetsmessige, beslutningsmessige, etiske og omdømmemessige sider av å betale løsepenger.

6. Rutiner for alternative kommunikasjonskanaler for hendelseshåndtering bør forberedes.

Etabler gode rutiner for sikkerhetskopiering og gjenoppretting:

1. Ha kontinuerlig oversikt over systemer som virksomheten må kunne gjenopprette i en krise. Juster beredskapsplaner deretter.
2. Opprettholde evne til å beskytte og gjenopprette sentral IKT-infrastruktur.
3. Opprettholde evne til å gjenopprette informasjon.
4. Ta sikkerhetskopi så ofte som virksomhetens behov tilsier.
5. Bestem hvor sikkerhetskopiene skrives til og lagres, og beskytt kopiene mot kapring.
6. Sikker drift av sikkerhetskopieringen.
7. Forbered virksomheten på evnen til å gjenopprette raskt.

Hindre at angriper kommer inn og sprer seg i virksomhetens systemer:

1. Tilgang til tjenester (og operativsystemet) bør ikke være ved bruk av enkle passord.
2. Ta i bruk web- og e-post-filtrering.
3. Sikkerhetsherde virksomhetens tjenester (inkludert operativsystemet til serveren den kjører på).
4. Ikke la tjenester være direkte tilgjengelig via internett.
5. Etabler tilgangskontroll på flest mulige nettverksporter i virksomhetens nettverk.
6. Etabler kontrollert dataflyt i virksomhetens nettverk.
7. Sperr all direkte-trafikk mellom klienter.
8. Regelmessig kartlegg og fjern «glemte» maskiner, tjenester og brukerkontoer.
9. Etabler hensiktsmessig systemovervåkning i nettverk og på klienter og servere.

Hindre kjøring av angripers programvare:

1. Ikke gi brukere administrator-rettigheter på klienten.
2. Vurder hvilke typer brukere som må kunne eksekvere alt av programvare.
3. Hindre at programvare i dokumenter blir eksekvert.
4. Alle klienter og servere bør driftes av virksomheten med et sentralisert driftsverktøy.
5. Fas ut eldre programvare (operativsystem og applikasjoner) og maskinvare som ikke lengre støttes av leverandør.
6. Fjern/deaktiver ubrukt funksjonalitet.
7. Etabler mest mulig automatisert sikkerhetsoppdatering av programvare.
8. Benytt skadevare-skanning (antivirus/antimalware) for å oppdage kjent skadevare.
9. Endre alle standardpassord på IKT-produktene.
10. Vurder om alle brukere må ha skriverett til alle fellesfiler.
11. Aktiver skadevarebeskyttelse som er innebygget i produkter og tjenester.

Håndtere hendelser med skadevare:

1. Informer alle berørte internt og eksternt, i tråd med ferdig planlagt kommunikasjonsstrategi.
2. Koble fra datamaskiner som er mistenkt infisert.
3. Vurder utkobling av deler av nettverk.
4. Vurdere passordbytte på alle kontoer på serverne og tjenester som er kompromittert.
5. På infiserte enheter bør man reinstallere all programvare.
6. Sjekk om fastvare er berørt.
7. Bruk kun sikkerhetskopier man er helt trygg på til gjenoppretting.
8. Gjenoppretting av enheter bør utføres på en del av nettverket man er trygg ikke er kompromittert.
9. Gjenoppta systemovervåkning av gjenopprettede enheter.
10. Lær av hendelsen.

Produktspesifikke råd:

1. Bruk sikkerhetsfunksjonalitet som er innebygget i operativsystemet.

OPPSUMMERING

Terskelen for kriminelle å ta i bruk ransomware-teknologi har blitt svært lav blant annet på grunn av "lønnsomme" verktøy som Ransomware-as-a-Service modellen. Ransomware vil derfor sannsynligvis forbli trussel nummer én de neste årene, og flere og flere enkeltpersoner og små/mellomstore bedrifter vil bli ofre for angrep. Dette gjør det desto viktigere å holde øye med trusselen ransomware utgjør, og være forberedt på alle eventualiteter.

En del ransomware-angripere har aldri tenkt å gi noen data tilbake. Andre har ikke implementert funksjonaliteten for dekryptering/datagjenoppretting på riktig måte, og det er de som ikke tester ransomware godt nok før den distribueres. Uansett, hvis du ikke har beskyttet deg godt nok mot ransomware, kan både penger og data gå tapt; og sjansen for at dette skjer er ikke ubetydelig.

Mange ransomware-hendelser kan unngås ved å iverksette grunnleggende sikkerhetstiltak. **Å forebygge er det mest effektive forsvaret mot ransomware**. Å alltid ha sikkerhetskopier av alle data og systemer er avgjørende for å kunne gjenopprette normal drift etter en hendelse. Gjenoppretting kan derimot være en kostbar, ressurs- og tidkrevende prosess som i tillegg kan kreve bistand fra en datagjenopprettingsspesialist, så det er derfor avgjørende å ta forholdsregler for å beskytte seg. Det er viktig med tilstrekkelig sikkerhetsbevissthet, og at brukerne er svært bevisste på hvordan de bruker sine enheter. Å beskytte mot infeksjon og spredning av skadevare med anti-malware, alltid holde alle systemer og programvare oppdaterte, herde alle servere og klienter, monitorering for å avdekke unormal aktivitet i systemene samt ha kontroll på bruker- og administrator-rettigheter, er alle svært viktige tiltak.

VEDLEGG 1 - MITRE ATT&CK MATRISE FOR RANSOMWARE-ANGREP