NSM

Erfaringer fra NSMs inntrengingstester:

Ti sårbarheter i norske IKT-systemer

Rapporten deler erfaringer fra NSMs inntrengingstester over tre år. Testene avslører ti vanlige sårbarheter. Les hvilke sikkerhetstiltak som anbefales med utgangspunkt i NSMs grunnprinsipper for IKT-sikkerhet.

15. november 2023

Nasjonal sikkerhetsmyndighet (NSM) er Norges direktorat for forebyggende nasjonal sikkerhet.

NSMs temarapporter inneholder råd og anbefalinger til bruk for norske virksomheter. De er ment å opplyse om temaer, bygge kompetanse og hjelpe norske virksomheter med forebyggende sikkerhetsarbeid.

Innhold

1 Formål med rapporten

Rapporten beskriver sårbarhetene NSM oftest finner under inntrengingstester av graderte og ugraderte informasjonssystemer. NSM videreformidler disse sårbarhetene slik at norske virksomheter kan lære om dem og håndtere dem. For hver av sårbarhetene presenterer NSM sikringstiltak med utgangspunkt i rådene i NSMs grunnprinsipper for IKT-sikkerhet.

2 Målgrupper

Rapporten henvender seg primært til personer som utvikler, kjøper inn, konfigurerer, sikrer og drifter informasjonssystemer i norske virksomheter.

3 Hva er inntrengingstesting?

Inntrengingstesting er kontrollerte dataangrep som prøver ut sikkerheten i informasjonssystemer. Testerne simulerer handlingene til en ondsinnet aktør. De gjennomfører praktiske, stikkprøvebaserte undersøkelser for å få kontroll over virksomhetens digitale miljøer og verdier, og dermed avdekke sårbarhetene som gjorde dette mulig. Testene foregår i en avgrenset tidsperiode og mot deler av systemene som nettverk og datamaskiner, samt fysiske lokasjoner. I dette inngår blant annet å avdekke manglende sikkerhetsoppdateringer, konfigurasjon av enheter og styring av nettverkstrafikk. Inntrengingstesting av fysiske lokasjoner avdekker forbedringspotensialer som forebygger at uvedkommende får tilgang. Inntrengingstester gir et øyeblikksbilde av de delene av informasjonssystemet som er omfattet av testen, men vil aldri gi et fullstendig bilde av status.

4 Hva gjør NSM?

NSM tilbyr inntrengingstester av informasjonssystemer og tilhørende fysiske lokasjoner hos norske virksomheter. Etter endt test får virksomheten en rapport som dokumenterer funn, sårbarheter og forslag til tiltak. NSM har drevet med inntrengingstesting i mange år og har opparbeidet seg betydelig kunnskap om hvilke sårbarheter norske virksomheter har i sine informasjonssystemer og hvordan disse lar seg utnytte. Selv om slike tester aldri er uttømmende så utnytter de sårbarheter innen en rekke områder, både tekniske og menneskelige. Fokuset er på svakheter innen oppbygning og drift av informasjonssystemene til forskjell fra klassifiseringer av programvaresårbarheter som CVE (Common Vulnerabilities and Exposures).

5 Oppsummering

Rapporten presenterer de ti vanligste sårbarhetene observert under NSMs inntrengingstester fra 2020 til 2022, samt tiltak for å håndtere dem. De fleste informasjonssystemer NSM møter er Windows-baserte, noe listen over sårbarheter gjenspeiler. Virksomhetene sårbarhetene er hentet fra, er underlagt sikkerhetsloven og hører blant annet hjemme i forsvarssektoren, justissektoren og sentralforvaltningen.

De ti sårbarhetene NSMs testere oftest finner i norske virksomheter er (ikke sortert):

1. Svake passord
2. Mulighet for å utføre passordgjettingsangrep
3. Uendrede standardpassord
4. Ubeskyttede passord og andre autentiseringsdata
5. Gamle, inaktive administratorkontoer
6. For høye rettigheter på og for bred bruk av administratorkontoer
7. Sårbar og utdatert programvare og protokoller
8. Ikke-støttede operativsystemversjoner
9. Mangelfull nettverkssegmentering og trafikkstyring
10. Mangelfull herding av informasjonssystemet

Flere av sårbarhetene over og årsakene deres har mye til felles. De fleste skyldes mangelfull oversikt over egne systemer og rutiner knyttet til passord- og brukerkontobehandling. Mange skyldes også manglende oppdateringer av programvare og feilkonfigurasjon av tjenester.

I rapporten følger en mer detaljert presentasjon av sårbarhetene, samt tiltak for å håndtere dem. Rapporten peker også til hvilke av NSMs grunnprinsipper for IKT-sikkerhet som er relevante for å lukke de enkelte sårbarhetene. NSM anbefaler alle norske virksomheter å følge grunnprinsippene. De kan hjelpe virksomheter i arbeidet med å bedre og prioritere IKT-sikkerheten i egne systemer.

Ytterligere informasjon:

- NSMs grunnprinsipper for IKT-sikkerhet (nsm.no): Råd for å beskytte informasjonssystemer, data og tjenester mot uautorisert tilgang, skade eller misbruk.
- Cyber Kill Chain (ekstern lenke, fra Lockheed Martin): Viser syv ulike stadier som ofte benyttes i forbindelse med cyberangrep.
- MITRE ATT&CK (ekstern lenke): Global kunnskapsdatabase som viser taktikker og teknikker som benyttes av trusselaktører i forbindelse med cyberangrep.

6 NSM ser de samme sårbarhetene år etter år

Tilbake i 2014 presenterte NSM en liste over fire tiltak som ville stoppe de fleste angrep som ble gjennomført over internett. Listen var ment å lukke de mest alvorlige sårbarhetene i informasjonssystemer. Disse tiltakene er tatt inn som en del av NSMs grunnprinsipper for IKT-sikkerhet, og siden oppdatert og endret til fem tiltak. Selv om NSM erfarer at norske virksomheter har et økt fokus på digital sikkerhet, er mange av de samme sårbarhetene som ble oppdaget for ti år siden fremdeles tilstede. NSM ser ofte at de viktigste tiltakene er mangelfullt tatt i bruk.

Virksomheter må ha en strategi og plan for å modernisere egne digitale plattformer og tjenester. Denne må være en integrert del av virksomhetens overordnede strategi og mål. Det tar ofte lang tid å bytte ut og endre digitale systemer, både for leverandører og brukere. For å kunne opprettholde en sikker plattform med effektive og sikre applikasjoner, må modernisering og videreutvikling være en naturlig del av virksomhetens arbeid. Nyere kontainerbaserte-plattformer, ofte omtalt som «cloud native», bør være en del av strategien.

Mange norske virksomheter har små driftsmiljøer. NSM har i mange år oppfordret norske virksomheter til å søke mot større, konsoliderte miljøer og mer profesjonell drift av digitale løsninger. Ofte vil dette være den eneste veien til et moderne og sikkert informasjonssystem. Slik kan man unngå digital gjeld og midlertidige løsninger og lukke de sårbarhetene som presenteres i denne rapporten.

Ytterligere informasjon:

- Statens muligheter for IT-modernisering og digital transformasjon (nsm.no): Om helhetlig og enhetlig digital modernisering og transformasjon i staten.
- Fem effektive tiltak mot dataangrep (nsm.no): Tiltak som systemeiere bør benytte for å beskytte sine systemer mot internett-relaterte, digitale angrep.

7 De ti sårbarhetene

7.1 Svake passord

De fleste virksomhetene NSM tester benytter kun brukernavn og passord for å autentisere seg, selv om det nå finnes flere alternativer. Svake passord av typen *Virksomhet1!* og *Sommer2023* florerer. Testerne ser sjelden passordregimer som oppfordrer til bruk av lange, gode passfraser som er enkle å huske. Vanskelige regler kombinert med hyppige passordskifter resulterer ofte i bruk av gjentatte tegnsekvenser, gule lapper med nedskrevne passord og gjenbruk på tvers av systemer. For NSM er det ofte nok å ha tilgang til virksomhetens nettverk for å kunne gjette passord (se 7.2 passordgjettingsangrep). Når NSM henter ut virksomhetenes passorddatabaser, knekkes normalt en stor andel av de krypterte passordene med spesialverktøy.

Når NSM gjetter eller knekker passordet til en brukerkonto, vil testerne ofte kunne operere som om de var denne brukeren. Dette kan gi både innledende tilgang til noen få tjenester, forhøyde rettigheter i nettet, eller til og med full kompromittering som domeneadministrator. Ofte gjøres dette ved hjelp av sideveis bevegelse i nettet.

Anbefalte tiltak

God passordsikkerhet er avhengig av at virksomheten har en god sikkerhetskultur. Virksomheten må etablere retningslinjer for tilgangskontroll og de ansatte må få opplæring for å følge retningslinjene. Det gjelder også de som drifter systemene. Informasjonssystemet må hindre brukerne i å velge svake passord, men altfor rigide og komplekse passordregimer virker ofte mot sin hensikt.

Virksomhetene bør innføre flerfaktorautentisering hvis mulig. Virksomhetene bør også forsøksvis redusere bruken av passord og gjerne tilby ansatte muligheten til å logge på maskiner med biometri der dette støttes. Hvis mulig, bruk *single-sign-on*- og FIDO-løsninger.

Relevante grunnprinsipper (nsm.no):

- 2.2 Etabler en sikker IKT-infrastruktur (se eksempelvis tiltak 2.2.1a)
- 2.6 Ha kontroll på identiteter og tilganger (se eksempelvis tiltak 2.6.1, 2.6.2, 2.6.3a, b, e og 2.6.7)

Ytterligere informasjon:

- Råd og anbefalinger om passord (nsm.no): Om både oppbygning og håndtering av passord.
- Sikkerhetskultur (nsm.no): Om atferd knyttet til sikkerhet rundt blant annet informasjon og objekter.
- FIDO-alliansen (ekstern lenke): Et samarbeid mellom flere virksomheter for å lage standarder for autentisering.

7.2 Passordgjettingsangrep

En bruker som ønsker å benytte en ressurs vil typisk be informasjonssystemet om tilgang basert på brukernavn og passord. Det skjer gjerne via Active Directory som er en sentral tjeneste i de aller fleste Windows-miljøer. Det er denne funksjonaliteten NSM utnytter ved passordgjettingsangrep. Testerne kombinerer en passordkandidat med mange eller alle brukernavnene i domenet og spør om tilgang til en ressurs. Passordet stemmer hvis domenekontrolleren gir tilgang.

Kun ett riktig gjettet passord er nok til at NSM kan få fotfeste hos en virksomhet. Det hender også at brukere med høyere rettigheter, inkludert domeneadministratorer, har passord som er så svake at de kan gjettes. Det er derfor i ytterste konsekvens mulig å gå fra ikke å ha noen andre rettigheter enn tilgang til virksomhetens nett, til å få full kontroll over informasjonssystemet ved målrettet gjetting av svake passord.

NSMs testere kan ofte utføre så hyppige spørringer at de får suksess med en innlysende passordkandidat (se 7.1 svake passord). NSMs testere opplever at slike massive mengder med spørringer sjeldent blir detektert og møter sjelden på flerfaktorautentiseringsløsninger.

Anbefalte tiltak

I tillegg til å gjøre tiltak rundt selve passordkvaliteten kan det gjøres grep knyttet til autentiseringsmekanismen. Virksomheten kan begrense hvor mange ganger brukere får lov til å skrive feil passord og hvor lenge brukeren i så fall nektes å prøve på nytt. Aktiviteten bør også overvåkes og flerfaktorautentisering innføres hvis mulig.

Relevante grunnprinsipper (nsm.no):

- 2.6 Ha kontroll på identiteter og tilganger (se eksempelvis tiltak 2.6.7)
- 3.2 Etabler sikkerhetsovervåkning (alle tiltak)
- 3.3 Analyser data fra sikkerhetsovervåkning (alle tiltak)

Ytterligere informasjon:

- Password spray investigation (ekstern lenke, fra Microsoft): Hvordan oppdage og håndtere passordgjettingsangrep
- Råd og anbefalinger om passord (nsm.no): Om både oppbygning og håndtering av passord.

7.3 Uendrede standardpassord

Mange tjenester, enheter og spesialkontoer er satt opp med standardpassord fra leverandørens side. Disse må endres. NSMs testere finner hyppige eksempler på det motsatte og klarer ofte å enten gjette passordene eller finne dem på nett ved hjelp av enkle søk, gjerne i offisiell brukerdokumentasjon. Om passordene er endret finner NSM dem ofte i felles passordlister på åpne filområder, på gule lapper eller direkte på utstyr (se 7.4 ubeskyttede passord og autentiseringsdata). NSM finner også at spesialkontoer har standardpassord etter krav fra leverandører.

Standardpassord er en særdeles enkel måte for NSM å få tilgang til en spesialkonto eller -tjeneste. Et fotfeste på en tjener eller en annen enhet, som skrivere, IoT-enheter og nettverksutstyr, vil senere kunne gi ytterligere tilganger. Bruk av standardpassord er spesielt uheldig på tjenester og enheter som er internett-eksponerte eller forvalter virksomhetens verdier.

Anbefalte tiltak

Virksomheten må ha gode rutiner og legge til rette for at standardpassord endres under konfigurasjon. Nye passord må beskyttes på en sikker og brukervennlig måte. Ved å kartlegge tjenester og filområder kan virksomheten oppdage om passord faktisk er skiftet og oppbevart på en sikker måte. Virksomheten bør være oppmerksom på leverandører som bruker samme standardpassord hos ulike kunder.

Relevante grunnprinsipper (nsm.no):

- 1.3 Kartlegg brukere og behov for tilgang (se eksempelvis tiltak 1.3.1 og 1.3.2)
- 2.2 Etabler en sikker IKT-infrastruktur (se eksempelvis tiltak 2.2.1a)
- 2.3 Ivareta en sikker konfigurasjon (se eksempelvis tiltak 2.3.7)
- 2.6 Ha kontroll på identiteter og tilganger (se eksempelvis tiltak 2.6.3e og 2.6.7)
- 3.1 Oppdag og fjern kjente sårbarheter og trusler (se eksempelvis tiltak 3.1.2)

Ytterligere informasjon:

- Risks of Default Passwords on the Internet (ekstern lenke, fra CISA): Informasjon om typiske tjenester og enheter som kan ha standardpassord, samt måter å håndtere sårbarheten på.

7.4 Ubeskyttede passord og autentiseringsdata

NSM finner ofte «passordhuskelister» hos alt fra IKT-drift til HR-personale. Passordene tilhører gjerne eksterne tjenester eller kontoer som deles mellom ansatte. Førstnevnte gjenbrukes ofte lokalt. Testerne ser passord på administratorkonti lagret på filområder som er lesbare for vanlige brukere – enten fordi disse lagres feil sted eller fordi brukerne har tilganger de ikke trenger. I noen tilfeller ligger det passord i kunnskapsdatabaser som ikke krever innlogging. NSM finner også eksempler på uheldig konfigurasjon hvor passord eller andre autentiseringsdata er lagret i klartekst i skript, konfigurasjonsfiler og kommandolinjehistorikk.

Denne sårbarheten er svært alvorlig. Uansett hvor langt og komplisert passordet er, hjelper det ikke hvis det lagres i klartekst. For NSM er ubeskyttede passord ofte en enkel vei til full kontroll over et informasjonssystem. Passord som lagres i klartekst tilhører gjerne administratorkontoer, noen ganger til og med domeneadministratorer. Delte kontoer har ofte like eller avledede passord, og hvis et passord blir kompromittert kan man få en dominoeffekt hvor mange andre kontoer følger. Ubeskyttede passord er gjerne nøkkelen til å bryte seg gjennom de sikkerhetssonene som er etablert i virksomheten.

Anbefalte tiltak

Virksomheten bør redusere bruken av delte passord og innføre systemer for sikker lagring av delte passord, samt introdusere flerfaktorautentisering der dette er mulig. For å unngå andre typer ubeskyttede autentiseringsdata, kan virksomheten herde systemene sine og følge med på publiserte sårbarheter. I begge tilfeller bør virksomheten vurdere å begrense både tilgangen til delte filområder og rettighetene til brukere etter prinsippet om minste privilegium.

Relevante grunnprinsipper (nsm.no):

- 1.1 Kartlegg styringsstrukturer, leveranser og understøttende systemer (se eksempelvis tiltak 1.1.5 og 1.1.6)
- 1.3 Kartlegg brukere og behov for tilgang (se eksempelvis tiltak 1.3.1)
- 2.6 Ha kontroll på identiteter og tilganger (se eksempelvis tiltak 2.6.7)
- 2.7 Beskytt data i ro og i transit (se eksempelvis tiltak 2.7.1)

Ytterligere informasjon:

- Råd og anbefalinger om passord (nsm.no): Om både oppbygning og håndtering av passord.

7.5 Gamle, inaktive administratorkontoer

Active Directory og tilsvarende tjenester deaktiverer ikke automatisk brukerkontoer som ikke lenger benyttes. NSMs testere går aktivt inn for å lete etter eldre administratorkontoer og finner ofte ut i ettertid at virksomheten ikke lenger kjenner til dem. Disse utgjør en helt unødvendig sikkerhetsrisiko. De viser seg ofte å ha kombinasjoner av rettigheter og gruppetilhørigheter som gjør dem ekstra verdifulle. I tillegg har de gjerne trivielle passord som ble satt før virksomheten innførte strengere passordkrav.

NSMs testere har skaffet seg tilgang til gamle kontoer som ligger i domeneadministratorgruppen ved å gjette trivielle passord, og støter fortsatt på passord lagret i det eldre, svært sårbare LM-formatet. Testerne vil typisk kunne benytte en slik ubrukt konto fritt straks de kjenner passordet.

Anbefalte tiltak

Virksomheten må forvalte brukerkontoene sine aktivt. Kontoer som ikke lenger er i bruk, må deaktiveres og systemrettigheter bør fjernes. Rettighetene til administratorkontoer bør begrenses etter prinsippet om minste privilegium og revideres jevnlig.

Relevante grunnprinsipper (nsm.no):

- 1.3 Kartlegg brukere og behov for tilgang (se eksempelvis tiltak 1.3.1 og 1.3.2)
- 2.2 Etabler en sikker IKT-infrastruktur (se eksempelvis tiltak 2.2.1a)
- 2.6 Ha kontroll på identiteter og tilganger (se eksempelvis tiltak 2.6.2 og 2.6.3)

7.6 For høye rettigheter på og for bred bruk av administratorkontoer

Mye av den digitale administrasjonen i en virksomhet må utføres via kontoer med forhøyede rettigheter. Disse er verdifulle mål og NSM angriper dem med teknikker som for eksempel overvåking, tastetrykkslogging, sesjonsstjeling og *hash*- eller passordavlesning.

Disse kontoene har ofte høyere rettigheter enn de trenger for å utføre driftsoppgaver, og mange spesialkontoer med begrensede bruksområder gis generelle rettigheter. Slike verdifulle kontoer brukes gjerne direkte på forskjellige tjenere på tvers av segmenteringen i virksomheten og er derfor utsatt for angrep.

NSMs angrep ender ofte med at testerne får tak i påloggingsinformasjonen til en eksponert bruker eller på annen måte klarer å kjøre kode i brukerkontoens kontekst. Testerne omgår dermed autentiseringsmekanismene i informasjonssystemet. Hvis kontoen som blir angrepet, tilhører en domeneadministrator eller tilsvarende får NSM ofte full kontroll over informasjonssystemet. Avlesning av kontohasher tilhørende domeneadministrator for bruk i «pass the hash»-angrep gir også stort utbytte. Passord til administratorkontoer blir ofte gjenbrukt og NSMs testere kan dermed få ytterligere gevinster.

Anbefalte tiltak

Administrator- og spesialkontoer bør kun ha rettigheter de har behov for til rollen. Bruken av slike kontoer bør begrenses til klart definerte deler av nettet og påloggingen bør kun skje på spesielt beskyttede maskiner.

Relevante grunnprinsipper (nsm.no):

- 1.1 Kartlegg styringsstrukturer, leveranser og understøttende systemer (se eksempelvis tiltak 1.1.5 og 1.1.6)
- 1.3 Kartlegg brukere og behov for tilgang (se eksempelvis tiltak 1.3.1 og 1.3.2)
- 2.2 Etabler en sikker IKT-infrastruktur (se eksempelvis tiltak 2.2.1a og 2.2.6)
- 2.6 Ha kontroll på identiteter og tilganger (alle tiltak)

Ytterligere informasjon:

- Enterprise access model (ekstern lenke, Fra Microsoft): Microsofts modell for inndeling og bruk av administratorkontoer.
- Securing devices as part of the privileged access story (ekstern lenke, fra Microsoft): Hvordan sette opp en arbeidsstasjon til bruk for administrasjon.
- Principle of least privilege (ekstern lenke, fra New Zealand CERT): Minste privilegiums prinsipp.

7.7 Sårbar og utdatert programvare og protokoller

All programvare inneholder feil. Det kan være alt fra designproblemer i en eldre protokoll til utnyttbare kildekodesårbarheter. Når en utnyttelse av en feil blir offentlig kjent, vil den bli publisert på nettet sammen med årsakene og eventuelle måter å håndtere den på. Leverandøren vil som oftest publisere en oppdatert versjon av programvaren. NSM kjenner til disse feilene og vet å utnytte dem. Testerne leter spesifikt etter tjenester som ikke er sikkerhetsoppdatert.

Spesialsystemer som IoT-enheter, nettverksutstyr og tjenester som er internett-eksponerte er spesielt utsatt. Mange virksomheter som NSM besøker har ikke faset ut utdaterte protokoller som ukryptert HTTP og eldre versjoner av for eksempel SMB og NTLM. I noen tilfeller krever eldre programvare at virksomheten enten åpner porter i brannmur, støtter utdaterte protokoller eller oppretter spesialkontoer med høye rettigheter. NSM ser ofte hvordan disse sårbarhetene forblir i informasjonssystemet selv om selve programvaren er fjernet.

Et enkelt nettverksangrep mot en sårbar tjeneste kan gi testerne mulighet til å avlytte trafikk, modifisere den eller kjøre egen kode med høye privilegier på en sårbar tjener. Slik får NSM muligheten til blant annet å bevege seg i nettet og til å forhøye rettigheter på den kompromitterte tjeneren. Testerne kan også få tilgang til passord og annen autentiseringsinformasjon for bruk i et neste steg.

Anbefalte tiltak

Virksomheten trenger en oversikt over all relevant programvare, som tjenester, operativsystemer og IoT- og nettverksutstyr. Denne oversikten må følges opp av rutiner for oppdateringer av programvare og utfasing av eldre, usikre protokoller. Virksomheten må følge med på sårbarhetspublikasjoner og ta grep hvis det oppdages sårbar programvare i informasjonssystemet. Ved å skanne nettet sitt vil virksomheten kunne oppdage både sårbare tjenester og uoverensstemmelser mellom oversikten og de faktiske forhold. Unntaksregler som er nødvendig for å kjøre eldre og spesialprogramvare, må fjernes når programvaren oppdateres. Eksempler på unntaksregler er åpne porter i brannmurer, støtte for utdaterte protokoller, eller krav om spesialkontoer med høye rettigheter.

Relevante grunnprinsipper (nsm.no):

- 1.1 Kartlegg styringsstrukturer, leveranser og understøttende systemer (se eksempelvis tiltak 1.1.5)
- 1.2 Kartlegg enheter og programvare (se eksempelvis tiltak 1.2.1, 1.2.2 og 1.2.4)
- 2.1 Ivareta sikkerhet i anskaffelses- og utviklingsprosesser (se eksempelvis tiltak 2.1.1, 2.1.2 og 2.1.9)
- 2.2 Etabler en sikker IKT-infrastruktur (se eksempelvis tiltak 2.2.1bc)
- 2.3 Ivareta en sikker konfigurasjon (se eksempelvis tiltak 2.3.1)
- 3.1 Oppdag og fjern kjente sårbarheter og trusler (se eksempelvis tiltak 3.1.1 og 3.1.2)

Ytterligere informasjon:

- Varsler fra NCSC (nsm.no): Nasjonalt cybersikkerhetssenter i NSM varsler blant annet om sårbarheter på internett, viktige oppdateringer og andre cyberhendelser.
- CVE - Common Vulnerabilities and Exposures (ekstern lenke): Klassifisering av programvaresårbarheter
- Retire Those Old Legacy Protocols (ekstern lenke, fra Microsoft): Informasjon om svakhetene ved noen mye brukte, utdaterte protokoller, samt hvordan man kan fjerne støtten for dem.

7.8 Ikke-støttede operativsystemversjoner

NSM ser ofte en eller flere tjenere som kjører operativsystemversjoner som er så gamle at det ikke blir publisert nye sikkerhetsoppdateringer til dem. Selv nyinnkjøpte spesialsystemer kan være utstyrt med slike operativsystemversjoner. Disse har gjerne utdaterte, sårbare tjenester som sjelden er herdet tilstrekkelig og mangler moderne sikkerhetsmekanismer. Denne sårbarheten er ofte mer alvorlig enn sårbar og utdatert programvare og protokoller (punkt 7.7) fordi det gjerne finnes ferdige oppskrifter for å utnytte kombinasjoner av sårbarheter i operativsystemet og medfølgende tjenester, noe som vil resultere i at en trusselaktør får full kontroll over tjeneren.

NSM er ofte hos virksomheter som må beholde gamle og utdaterte tjenere fordi de er avhengige av eldre applikasjoner som må kjøre på eldre utgaver av operativsystemet. NSM opplever at selv om virksomhetene er klar over risikoen disse tjenerne representerer, så gjøres det sjelden grep for å beskytte installasjonene, nettverket rundt, brukere eller andre deler av informasjonssystemet.

NSM vil typisk kunne få full kontroll over en slik eldre tjener og får dermed mulighet til å etablere fotfeste i virksomheten. Avhengig av informasjonssystemets oppbygning får testerne mulighet til å bevege seg i nettverket og nyttiggjøre seg av data på tjeneren, inkludert å angripe andre brukere og tilkoblinger.

Anbefalte tiltak

Virksomheten trenger en oversikt over alle operativsystemer i informasjonssystemet sitt og må så langt det er mulig sørge for at det kun brukes systemer som fortsatt får sikkerhetsoppdateringer fra leverandøren. Denne oversikten og status på oppdateringer bør verifiseres gjennom skanning av informasjonssystemet. Utdaterte operativsystemer som ikke kan oppdateres, bør kun brukes til sine spesielle oppgaver. De bør herdes spesielt og isoleres både fra og mot resten av informasjonssystemet via for eksempel segmentering og bruksmønster.

Relevante grunnprinsipper (nsm.no):

- 1.1 Kartlegg styringsstrukturer, leveranser og understøttende systemer (se eksempelvis tiltak 1.1.5)
- 1.2 Kartlegg enheter og programvare (se eksempelvis tiltak 1.2.1, 1.2.2 og 1.2.4)
- 2.2 Etabler en sikker IKT-infrastruktur (se eksempelvis tiltak 2.2.1e)
- 2.3 Ivareta en sikker konfigurasjon (se eksempelvis tiltak 2.3.1)
- 3.2 Etabler sikkerhetsovervåkning (alle tiltak)
- 3.3 Analyser data fra sikkerhetsovervåkning (alle tiltak)

Ytterligere informasjon:

- Risikovurdering av IKT-systemer (nsm.no): Guide til risikovurdering basert på NSMs grunnprinsipper for IKT-sikkerhet

7.9 Mangelfull nettverkssegmentering og trafikkstyring

Virksomheter bør dele nettet sitt inn i mindre, logiske nettverk av både ytelses- og sikkerhetsgrunner. Særlig bør virksomheter isolere de segmentene hvor administratorer, tjenere og/eller verdifull informasjon er plassert. Dette skaper utfordringer for NSMs testere som gjerne først får fotfeste i mer utsatte deler av nettet, som klient- og gjestenettverk.

Hvis det derimot er mulig med en relativ åpen kommunikasjon mellom forskjellige deler av nettet, kan NSM operere mer eller mindre fritt. I ytterste konsekvens kan testerne skanne alle porter på alle tjenere i virksomheten, inkludert domenekontrollere. Manglende segmentering kan også gi potensielle innsidere tilganger de ikke er autorisert for.

Anbefalte tiltak

Før virksomheten gjennomfører segmentering, må den ha oversikt over alle komponentene i informasjonssystemet og se sammenhengen mellom ressurser, verdier, tjenester og bruksmønstre. Dette vil gjøre virksomheten i stand til å ta i bruk en presis, finkornet og restriktiv segmentering som ikke forstyrrer den daglige driften.

Relevante grunnprinsipper (nsm.no):

- 1.1 Kartlegg styringsstrukturer, leveranser og understøttende systemer (se eksempelvis tiltak 1.1.5 og 1.1.6)
- 1.2 Kartlegg enheter og programvare (se eksempelvis tiltak 1.2.1, 1.2.3 og 1.2.4)
- 2.1 Ivareta sikkerhet i anskaffelses- og utviklingsprosesser (se eksempelvis tiltak 2.1.1 og 2.1.9)
- 2.2 Etabler en sikker IKT-infrastruktur (se eksempelvis tiltak 2.2.1g, 2.2.3, 2.2.4, 2.2.5 og 2.2.7)
- 2.4 Beskytt virksomhetens nettverk (alle tiltak)
- 2.5 Kontroller dataflyt (alle tiltak)
- 2.6 Ha kontroll på identiteter og tilganger (se eksempelvis tiltak 2.6.6)
- 2.7 Beskytt data i ro og i transitt (se eksempelvis tiltak 2.7.2, 2.7.4 og 2.7.5)
- 3.1 Oppdag og fjern kjente sårbarheter og trusler (se eksempelvis tiltak 3.1.1 og 3.1.2)

Ytterligere informasjon:

- Network infrastructure security guide (ekstern lenke, fra NSA): Sikring av eksisterende nettverk.
- Zero trust architecture design principles (ekstern lenke, fra NCSC UK): Zero trust er en sikkerhetstilnærming som flytter fokus fra perimetersikring til å sikre de enkelte ressurser eller grupper av ressurser i systemet.

7.10 Mangelfull herding av informasjonssystemet

En virksomhet vil typisk ha et mangfold av tjenester, enheter, protokollimplementasjoner, operativsystemer og nettverk i egne digitale miljøer. Felles for disse er at de må herdes, altså konfigureres for sikkerhet, i tillegg til funksjonalitet og ytelse.

En mangelfull herdet enhet er ofte et svakt punkt hos virksomheten. Ofte er ikke virksomheten klar over at enheten fortsatt er tilkoblet informasjonssystemet. NSM får gjerne gevinst ved å enumerere og analysere alle tilgjengelige systemer, og angripe de som er sårbare. Veldig ofte opplever testerne at teknikker kun fungerer fordi målet ikke var herdet: En protokoll tillot nedgradering, en sikkerhetsmekanisme var ikke slått på, eller en endepunktssikkerhetsplattformen (antivirus) var ikke korrekt konfigurert eller oppdatert.

Et system som ikke er herdet kan gjøre alt fra å a) lekke informasjon om det digitale miljøet, b) tillate elevering og bevegelse i nettverket, c) gjøre det mulig for et løsepengeangrep å spre seg og skape store ødeleggelser, til å d) tillate fullstendig kompromittering. Dette vil avhenge av hvilket system som kompromitteres, hvilken konkret sårbarhet som utnyttes og informasjonssystemets øvrige oppbygning.

Anbefalte tiltak

Herding er en helhetlig prosess hvor sikring av applikasjoner, operativsystemer, databaser, maskinvare og nettverk inngår. Flere av sårbarhetene beskrevet tidligere kunne vært unngått med riktig herding. Virksomheten må ha en oversikt over alle digitale systemer og bør forsikre seg om at spesialsystemer blir inkludert. NSMs grunnprinsipper for IKT-sikkerhet beskriver god praksis for sikring av IKT-systemer, inkludert herding. NSMs fem effektive tiltak tar frem noen av de viktigste av disse igjen og bør være blant de mest prioriterte for virksomhetene (se kapittel 6 for ytterligere beskrivelse).

Relevante grunnprinsipper (nsm.no):

- 1.1 Kartlegg styringsstrukturer, leveranser og understøttende systemer (se eksempelvis tiltak 1.1.5 og 1.1.6)
- 1.2 Kartlegg enheter og programvare (se eksempelvis tiltak 1.2.1, 1.2.2, 1.2.3 og 1.2.4)
- 2.1 Ivareta sikkerhet i anskaffelses- og utviklingsprosesser (se eksempelvis tiltak 2.1.1, 2.1.2 og 2.1.9)
- 2.2 Etabler en sikker IKT-infrastruktur (se eksempelvis tiltak 2.2.1 og 2.2.7)
- 2.3 Ivareta en sikker konfigurasjon (alle tiltak)
- 2.6 Ha kontroll på identiteter og tilganger (se eksempelvis tiltak 2.6.7)
- 2.7 Beskytt data i ro og i transitt (se eksempelvis tiltak 2.7.2 og 2.7.4)
- 2.8 Beskytt e-post og nettleser (alle tiltak)
- 3.1 Oppdag og fjern kjente sårbarheter og trusler (se eksempelvis tiltak 3.1.1 og 3.1.2)
- 3.2 Etabler sikkerhetsovervåkning (alle tiltak)
- 3.3 Analyser data fra sikkerhetsovervåkning (alle tiltak)

Ytterligere informasjon:

- Device Security Guidance (ekstern lenke, fra NCSC UK): Guide til herding av informasjonssystemer.

- Windows Defender Application Control and AppLocker Overview (ekstern lenke, fra Microsoft): Hvordan man kan begrense kjøring av uautorisert kode.