NORMEN

Passord og passordhåndtering

Faktaark 31

Versjon 3.0

Juni 2023

Utarbeidet med støtte fra Direktoratet for e-helse

Vedtatt av styringsgruppen for Normen

Dette faktaarket er et støttedokument under Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen) som forvaltes av Styringsgruppen for Normen etter Normens forvaltningsmodell. Se mer på www.normen.no

Tema for faktaarket	Dette faktaarket omhandler passord og passordhåndtering. Formålet med faktaarket er å gi veiledning i hvordan virksomheten kan sikre at passord som benyttes i virksomheten er underlagt tilstrekkelig sikring. Faktaarket har en praktisk tilnærming og inneholder beste praksis knyttet til passord og passordhåndtering.
Dette faktaarket er spesielt relevant for	Målgruppen for faktaarket er virksomheter som behandler helse- og personopplysninger. Faktaarket er relevant for alle roller i virksomheten.
Krav i Normen	Faktaarket gjelder følgende kapitler i Normen - Kapittel 5.2.2 Autentisering
Relevante lov- og forskriftsbestemmelser, standarder og andre rammeverk	Følgende lov- og forskriftsbestemmelser, standarder og andre rammeverk er spesielt relevante for faktaarket: - Pasientjournalloven § 22 - NSMs grunnprinsipper for IKT-sikkerhet 2.0 - NIST 800-63b Digital Identity Guidelines - Selvdeklarasjonsforskriften kapittel 2

Om faktaarket

Passord benyttes fortsatt i utstrakt grad som ett av de mest brukte autentiseringskriterier for å sikre Normens krav til autentisering. Selv om passord alene ikke alltid gir tilstrekkelig sikker autentisering, er det viktig å sikre at passordene man benytter er gode og sikre, og at virksomheten har rutiner og prosedyrer for passordhåndtering. Passord skal ikke enkelt la seg misbruke, og skal håndteres på en slik måte at de ikke gjøres kjent for uvedkommende.

Faktaarket gir råd om passordpolicy basert på blant annet følgende kilder:

- Av truslene som beskrives av MITRE for dette tiltaket (Password Policies, Mitigation M1027 – Enterprise | MITRE ATT&CK®), så søker policyen primært å dekke området T1110 – "brute force"
- For listen hos NIST, jf. tabell 8.2 med tilhørende veiledning dekkes "offline cracking" og "online guessing".

Utvalget er basert på at veiledningsbehovet antas være størst når det gjelder krav som påvirker brukeropplevelsen. Dette omhandler hvordan passord skal utformes/velges, utestenging, nullstilling og passordbytte. Det er også tatt med forhold hvor det erfaringsmessig har vært uheldig praksis (passordlagring, krav til passordbytting).

Avgrensning

Faktaarket omhandler **passord** som autentiseringsmekanisme for brukere, og ikke passord brukt i andre sammenhenger som f.eks. ved kryptering eller maskin- til maskin-kommunikasjon. Faktaarket stiller ingen konkrete krav til passord, men gir en anbefaling basert på beste praksis.

Faktaarket beskriver ikke generelle krav til autentisering (f.eks. tofaktorautentisering), identitets- eller tilgangsstyring, men kommer med noen anbefalinger. Se eget avsnitt med henvisning til relevant veiledning om tilstøtende områder.

Hva sier Normen om krav til passord?

Normen stiller ikke faste krav til passord, men passord vil gjerne være en del av autentiseringsmekanismen (jf. Normen pkt. 5.2.2 Autentisering) som benyttes for å få tilgang til helseopplysninger (jf. Normen pkt. 5.2.1.2 Tilgang til helse- og personopplysninger mellom virksomheter). Som sikker autentiseringsløsning regnes en "autentiseringsløsning som gjennom en risikovurdering viser at den har tilstrekkelig sikkerhet".

I vurderingen av hva som gir tilstrekkelig sikker autentisering, vil det være en rekke relevante faktorer:

- Grad av fysisk sikring og kontroll på området der tilgangen gjøres fra.
- Skadepotensialet og angrepsflaten en eventuell uautorisert tilgang medfører, som f.eks. type data eller hvilke angrepsflater som tilgjengeliggjøres gjennom tilgang.
- Graden av tilgang/pålogging fra eksterne nett.
- Graden av intern nettverkssikring i åpne og lukkede soner. Med det menes at tilgang fra sikrede nett som virksomheten har kontroll over kan være et tiltak som kan ligge til grunn for at man vurderer å bruke svakere autentisering.

Trusler mot passord

Det finnes en rekke ulike trusler mot passord, hvor noen av de mest vanlige er:

Phishing
Bruker blir lurt til å gi fra seg passord gjennom f.eks. falske nettsider eller annen form for sosial manipulering.

Passordspraying
Angriper bruker kjente eller ofte benyttede passord mot mange brukerkontoer i et forsøk på å logge på en bruker. Dette kan f.eks. gjøres ved hjelp av lister over kjente passord.

Offline brute force - lekkede passord
Angriper har fått tilgang til ett eller flere krypterte passord, og kan bruke dette til å gjette med uttømmende søk eller et svært høyt antall passord. Dette kan f.eks. være passord som stammer fra tidligere angrep hos en leverandør, der passorddatabasen har havnet på avveie.

De to viktigste tiltakene mot at passord gjettes av en angriper er å hindre at angriper kan gjøre raske, gjentatte forsøk på å gjette passordet, og påse at passordet ikke er blant de som er lettest å gjette. Lange passord eller krav til sammensetning hjelper ikke dersom passordet allerede står i en ordliste. Vær oppmerksom på at det finnes ordlister som inneholder noen milliarder tegnsammensetninger som er brukt som passord. Det må forventes at disse forsøkes tidlig i passordangrep. Å prøve alle mulige passord på 6 tegn tar lengre tid enn å prøve 1 milliard passord fra en ordliste. Det finnes over 250 milliarder kombinasjoner av 6 tegn (her basert på 80 mulige tegn, f.eks. A-å, 0-9 og 12 symboler). System som er beskyttet mot hurtig gjetting, eksempelvis at det legges inn forsinkelser eller sperring etter et antall feilaktige forsøk, vil være mer motstandsdyktig mot denne typen angrep enn system uten slik beskyttelse. Derfor kan det være akseptabelt med PIN-koder med kun tall som passord for pålogging til enheter, der det kun tillates et lite antall påloggingsforsøk før enheten sperres.

Prosedyre for passord og passordhåndtering

Virksomheten skal utarbeide prosedyrer for passord og passordhåndtering. Rutinene skal beskrive krav til passord, krav til hvordan passord brukes og hvordan passord forvaltes.

Krav til passord må tilpasses risiko og omstendighetene ellers.

Passord kan brukes alene eller sammen med andre autentiseringsfaktorer for å få tilgang til systemer eller ressurser. Om det er forsvarlig å bruke passord alene, eller om det skal kreves flere faktorer, vil bero på omstendighetene.

Hensyn ved utforming av passordpolicy

a) Krav til autentiseringsstyrke, ref. det som omtales i "Hva sier Normen om krav til passord".
b) Passord skal bare være kjent for eier av bruker-ID.
c) Prosedyrene for utsteding av passord må inkludere:
    - Rutine for sikker tildeling og nullstilling av passord.
    - Passord skal ikke oppgis uten at det er trygghet for at det er den rette personen som får oppgitt passordet.
    - At passord ikke skal deles på e-post, SMS, via telefon eller lenker (unntak for engangspassord ved første gangs tildeling av passord).

Krav til bruk av passord

a) Utlån av passordet til andre personer er ikke tillatt.
b) Det skal være prosedyrer for hendelsesorientert bytte av passord. For eksempel hvis det er mistanke om at passordet er kommet på avveie eller at en risikovurdering indikerer behov for nye krav til passord.
c) Passord bør ikke gjenbrukes på tvers av ulike systemer. Spesielt viktig er det å skille på passord brukt på jobbrelaterte tjenester og passord brukt privat.

Gode råd for passordhåndtering

- Utfordringen med mange ulike passord kan håndteres gjennom å tilrettelegge for tilpassede verktøy for passordhåndtering.
- Bruk alltid flerfaktor-autentisering. Flerfaktor-autentisering er et effektivt tiltak dersom passord kommer på avveie, og kan dermed forhindre tilgang til og misbruk av informasjon og systemer. Det er imidlertid viktig å ha rutiner eller systemer som gir tilstrekkelig tilgjengelighet hvis flerfaktor-autentisering feiler.
- Passord benyttet til jobbrelaterte formål skal ikke benyttes til private tjenester.
- Bytt passord ved første gangs pålogging dersom passordet er tildelt av systemet eller andre personer (f.eks. administrator).
- Benytt egne verktøy for lagring og håndtering av passord. Valg av verktøy skal gjøres basert på en risikovurdering, og tilbys av virksomheten.
- Et alternativ til egne verktøy for passordhåndtering er å skrive ned passordet, men da må man sikre at passordene oppbevares trygt og separat.
- Benytt tilgjengelige tjenester for å sjekke om passordet har havnet på avveie. Ett eksempel på slike tjenester er https://www.haveibeenpwned.com
- Etabler gode rutiner for håndtering av avglemte passord og sperrede kontoer for å sikre tilgjengelighet til systemene. Dette kan blant annet innebære sikre selvbetjeningsportaler for gjenoppretting av konto og/eller passord.

Eksempel på gode passord

Gode passord trenger ikke å være komplekse eller vanskelig å huske. For strenge krav til selve passordet er beviselig en kilde til at brukere velger dårlige passord.

- Benytt lange passord heller enn komplekse passord, gjerne minst 15 tegn.
- Der systemer kun legger til rette for bruk av PIN, bør det settes krav til minimum 6 tegn.
- Bruk setninger som passord for enklere å kunne huske passordet.
- Dersom systemet ikke støtter lange passord, bør krav til passordkompleksitet settes ut fra vurdert risiko.
- Ikke benytt passord som inneholder ord eller tema som lett lar seg gjette. Dette kan være ord som er knyttet til deg, info om deg som er kjent, f.eks. adresse, navn på slektninger eller kjæledyr, bilmerke osv.

Håndtering av passord i systemene

Retningslinjene som settes til passord må håndheves, og dette kan gjøres på teknisk nivå (systemene selv) eller på organisatorisk nivå(virksomhetens prosedyrer og rutiner).

- Steng eller midlertidig steng konto ved gjentatte feilede forsøk på innlogging, f.eks. etter fem forsøk. Tiltaket bør sees i sammenheng med risikoen av å stenge en konto. Sikre løsninger for tilbakestilling av passord og konto er eksempler på tiltak som kan ta ned denne risikoen.
- Tilrettelegg for bruken av passordhåndteringsverktøy, f.eks. ved å la verktøyene lime inn passord.
- Tillat bruker å kunne vise inntastet passord, men skjul inntastingen som standard.
- Passord skal ikke måtte byttes med mindre det er bekreftet eller mistanke om at passordet er på avveie eller beslutninger på virksomhetsnivå tilsier at det skal byttes.
- Det bør ikke stilles krav om spesialtegn og store/små bokstaver i passordet.
- Der det er mulig bør det etableres automatisk sjekk av passord for å kunne avdekke svake passord. Det er hensiktsmessig at slike tiltak etableres i sentraliserte autentiseringsløsninger, som f.eks. Active Directory (AD).
- Bytt alltid standard-passord på utstyr.
- Det bør etableres systemer som kan avdekke og varsle ved misbruk av passord.
- Der det er mulig bør det legges til rette for Single Sign On (SSO), som forenkler innloggingen for brukere som benytter mange ulike systemer.
- Det bør etableres tvunget passordbytte hvis passord gjøres kjent for andre, f.eks. gjennom tildeling av førstegangspassord.
- Dersom systemet ikke støtter lange passord, bør krav til passordkompleksitet settes ut fra vurdert risiko.

Autentisering uten bruk av passord

Det finnes flere løsninger for passordfri autentisering. Dette er autentiseringsløsninger som benytter andre autentiseringskriterier som f.eks. FIDO2-nøkkel, Windows Hello med biometri (ansiktsgjenkjenning, fingeravtrykk mv.), og Authenticator app på mobiltelefon.

Fordelen med denne typen autentisering er at bruker ikke trenger å forholde seg til passord, og autentiseringen kan enkelt tilfredsstille kravene til sikker autentisering. Flere av løsningene som tilbys kan integreres med tillitstjenester på eIDAS-nivå Høy og Betydelig.

Dette vil igjen kunne åpne for enklere tilgang på tvers av virksomheter og landegrenser, da autentiseringsløsningene bygger på felles tillitsmodell og rammeverk.

Løsningene kan kreve en større teknisk tilrettelegging enn tradisjonell autentisering. Ved bruk av biometriske løsninger må det også vurderes hvordan personvernet ivaretas.

Avvik til passordanbefalinger

Ikke alle systemer kan understøtte anbefalingene i dette faktaarket. I de tilfellene systemet i seg selv setter slike begrensninger er det viktig at virksomheten håndterer dette særskilt.

- Still klare krav i anskaffelse av nye tjenester, slik at virksomhetens krav til passord kan oppfylles.
- Der systemer ikke tilfredsstiller kravene skal virksomheten, basert på en risikovurdering, etablere øvrige tiltak som sikrer tjenesten.

Kompletterende veiledningsmateriell

For en kompletterende veiledning til dette faktaarket kan det være særlig aktuelt å se på følgende kilder:

- Nasjonal sikkerhetsmyndighets (NSM) grunnprinsipper for IKT-sikkerhet 2.0 - grunnprinsipp 2.6 med tilhørende tiltak gir veiledning til helhetlig identitets- og tilgangsstyring. Ha kontroll på identiteter og tilganger - Nasjonal sikkerhetsmyndighet
- Råd og anbefalinger om passord – Nasjonal sikkerhetsmyndighet (nsm.no) og Passordråd for personer og virksomheter – Nasjonal sikkerhetsmyndighet (nsm.no)
- For konkrete anbefalinger knyttet til passordstyrke kan NIST 800-63b Digital Identity Guidelines være en god kilde. NIST Special Publication 800-63B
- For dypere forståelse for angrep mot passord kan informasjonen hos MITRE være nyttig.
- I tyske IT Grundschutz 2022 dekkes ORP.4.A8 (jf G0.18, 23, 29), A13 (aut.mekanisme - dekkes neppe), A22 (passordkvalitet, G0.18, 23, 29), A23 (passordhåndterer), se kryssreferanse og kompendium.