disnova
DISTRIBUTION

ManageEngine
PAM360

Grunnleggende privilegert tilgangsstyring for å forberede virksomheten på NIS2-direktivet

hei@disnova.no
+47 359 74 400

Om PAM360

PAM360, ManageEngines enterprise PAM-pakke, er en komplett sikkerhetsløsning for privilegert tilgang som hjelper IT-team med å håndheve streng styring av tilgangsveier til kritiske virksomhetsressurser. Med en helhetlig tilnærming til sikkerhet for privilegert tilgang dekker PAM360 kjernekravene til PAM og legger til rette for kontekstuell integrasjon med flere andre IT-administrasjonsverktøy. Resultatet er dypere innsikt, mer meningsfulle vurderinger og raskere tiltak. Mer enn 5 000 organisasjoner globalt og over 1 million administratorer stoler på PAM360 for
sine PAM-behov. Du kan lese mer om PAM360 og løsningens enterprise-klare funksjoner på https://mnge.it/pam360.

Introduksjon

NIS-direktivet (Network and Information Security) ble etablert av EU i 2016 som svar på flere høyprofilerte og skadelige cyberangrep. NIS2 skal styrke sikkerhetskravene, forenkle rapporteringspliktene og innføre strengere tilsynstiltak. Det oppdaterte NIS2-direktivet er utformet for å beskytte kritiske virksomheter bedre mot sårbarheter i leverandørkjeden, løsepengevirus og andre cybertrusler. Alle EU-medlemsstater er pålagt å innarbeide NIS2-direktivet i nasjonalt regelverk innen oktober 2024.

Dette dokumentet beskriver betydningen av privilegert tilgangsstyring i sammenheng med NIS2-direktivet, inkludert fordeler, implementeringsstrategier og beste praksis.

NIS2: Hva er nytt?

NIS2bygger videre på NIS-direktivet fra 2016 ved å utvide omfanget og innføre strengere sikkerhetstiltak. Direktivet skal styrke cybersikkerheten hos vesentlige og viktige virksomheter i en rekke sektorer, blant annet energi, transport, avfalls- og avløpshåndtering, produksjon med mer. Utover disse kjerneområdene gjelder NIS2 også for flere typer virksomheter, inkludert nettbaserte markedsplasser, offentlige forvaltningsorganer og posttjenester.

NIS2-direktivet skal forbedre sikkerheten og motstandsdyktigheten i nettverks- og informasjonssystemer i hele EU. De viktigste målene er:

1. Forsterkede cybersikkerhetstiltak
Pålegger robuste cybersikkerhetsrutiner for vesentlige og viktige virksomheter.

2. Hendelsesrapportering
Krever rask rapportering av vesentlige hendelser til nasjonale myndigheter.

3. Sikkerhet i leverandørkjeden
Sikrer at leverandører og tjenesteytere opprettholder tilstrekkelige sikkerhetstiltak.

4. Harmonisering
Standardiserer cybersikkerhetspraksis på tvers av medlemsstatene for mer ensartet beskyttelse.

Direktivet understreker behovet for helhetlige sikkerhetsrammeverk, inkludert beskyttelse av privilegerte kontoer og tilganger, som ofte er mål for cyberangripere.

Betydningen av privilegerte kontoer i sammenheng med NIS2-direktivet

Privilegerte kontoer er brukerkontoer med utvidede rettigheter i et system. De kan gi tilgang til kritisk infrastruktur, sensitive data og mulighet til å endre systemkonfigurasjoner. Slike kontoer er attraktive mål for cyberkriminelle, fordi kompromittering kan få alvorlige konsekvenser. NIS2 understreker behovet for robuste kontroller for privilegert tilgang for å redusere denne risikoen.

Privileged access management, eller PAM, handler om å overvåke og styre kontoer med utvidede rettigheter. Hvis slike kontoer kompromitteres, kan det føre til alvorlige sikkerhetsbrudd. PAM-kontroller er derfor avgjørende for å sikre kontoene og sørge for at tilgangen både er autorisert og overvåket.

Viktige komponenter i PAM

Flere sentrale bestemmelser i NIS2 samsvarer direkte med kjerneområdene i privilegert tilgangsstyring. Slik bidrar PAM til å oppfylle NIS2-kravene:

- Risikostyring og hendelsesrapportering
NIS2 anbefaler en risikobasert tilnærming for å identifisere og håndtere cybersikkerhetsrisiko. PAM-løsninger tilbyr omfattende funksjoner for risikovurdering som avdekker sårbarheter knyttet til privilegert tilgang.

- Risikovurderingsfunksjoner bidrar til å identifisere sårbarheter knyttet til privilegert tilgang. I tillegg gir PAM detaljert logging og sesjonsopptak, noe som gjør hendelsesundersøkelser og rapportering mer effektivt, slik NIS2 legger opp til.

- Tilgangsstyring
NIS2 legger vekt på strenge tilgangskontroller, slik at brukere bare har de minste rettighetene de trenger for å utføre oppgavene sine. PAM håndhever prinsippet om minste privilegium og JIT-tilgang ved å gi detaljert tilgang basert på roller, tilgangspolicyer og behov. Dette begrenser skadeomfanget hvis legitimasjon blir kompromittert.

- Zero Trust-tilgang (MFA og adaptiv tilgang)
NIS2 fremhever betydningen av MFA for å styrke autentisering. PAM-løsninger integreres sømløst med MFA-systemer og gir et ekstra sikkerhetslag utover passord.

- Kontoadministrasjon
NIS2 anbefaler robuste rutiner for kontoadministrasjon, inkludert regelmessig passordbytte og overvåkning av privilegerte sesjoner. PAM automatiserer passordrotasjon og håndhever tidsavbrudd for sesjoner, slik at angripernes handlingsrom reduseres. PAM gir også sanntidsovervåkning av privilegerte sesjoner.

- og gjør det mulig å oppdage mistenkelig aktivitet.

- Sikkerhet i leverandørkjeden
NIS2 fremhever viktigheten av å sikre leverandørkjeden. PAM-løsninger kan også brukes til å styre privilegert tilgang for tredjepartsleverandører og konsulenter, slik at tilgang til kritiske systemer og data er sikker.

Et helhetlig PAM-program kan hjelpe virksomheter med å styrke sikkerheten, øke kontrollen over sensitive endepunkter og ressurser, og forbedre NIS2-beredskapen innen tilgangsstyring.

Hvordan ManageEngine PAM360s helhetlige kontroller bidrar til samsvar med NIS2-direktivet

Cybersikkerhetstiltakene i artikkel 21 i NIS2-direktivet krever at virksomheter tar en helhetlig og altomfattende tilnærming til cybersikkerhet. Dette innebærer å beskytte både nettverks- og informasjonssystemer og de fysiske miljøene. Det omfatter tiltak for hendelseshåndtering, kontinuitet, sikkerhet i leverandørkjeden og policy for risikoanalyse.

I tillegg bør virksomhetene fremme grunnleggende cyberhygiene og cybersikkerhetsopplæring, styre bruk av kryptografi og håndheve sikkerhet for ansatte og tilgangskontroll. Bruk av flerfaktorautentisering og sikker kommunikasjon fremheves også der det er relevant.

NIS2-direktivet inneholder også detaljerte avsnitt som beskriver mål, intensjoner og motivasjon bak direktivet.

NIS2-avsnitt	Relevante PAM-kontroller og beste praksis	Hvordan PAM360 hjelper
Artikkel 21, 2(d): Sikkerhet i leverandørkjeden, inkludert kritisk infrastruktur		
53: Sikkerhet i forsynings- og infrastruktursektoren	Etter hvertsom byer blir smartere og forsyningstjenester i økende grad baserer seg på digitale nettverk for transport, vann, avfall og energi, blir de mer sårbare for cyberangrep. Slike angrep kan få store samfunnsmessige konsekvenser fordi smarte bysystemer henger tett sammen. Medlemsstatene bør derfor ta inn policyer som håndterer cybersikkerhetsrisiko i smarte byer i sine nasjonale strategier.	- PAM360 tilbyr et robust sett med kontroller som er bygget for å beskytte smarte bymiljøer. Løsningen reduserer cyberrisiko ved å isolere privilegerte sesjoner, håndheve JIT-tilgang og styre legitimasjon strengt på tvers av distribuerte forsyningsnettverk. Ved å fjerne permanente privilegier og gi detaljert kontroll reduserer PAM360 angrepsflaten i tilkoblede urbane systemer. - PAM360 bruker også identitetssikkerhetsintelligens for å oppdage avvikende atferd som kan indikere cyberangrep. Dette gir tidlig oppdagelse og rask respons. Endpoint privilege security fjerner lokale administratorrettigheter på enheter i forsyningsinfrastrukturen og begrenser uautorisert programatferd.

NIS2-avsnitt	Relevante PAM-kontroller og beste praksis	Hvordan PAM360 hjelper
		- Sammen med sterke funksjoner for identitets- og tilgangsstyring, som sikker passordhvelving og phishing-resistente kontroller, gjør PAM360 det mulig for byadministratorer å styre digital tilgang sikkert, beskytte kritisk infrastruktur og sikre uavbrutt levering av samfunnskritiske tjenester.
54: Beskyttelse mot løsepengevirus	Virksomheter kan vurdere å: - innføre en kontroll som fjerner lokale administratorkontoer fra endepunkter for å hindre spredning av løsepengevirus. - bruke en policybasert tilgangsmodell for å tillate eller nekte hvilke programmer som kan kjøres på endepunkter basert på egenskaper, leverandør osv.	- PAM360s modul for endpoint privilege management hjelper administratorer med å trekke tilbake lokale administratorrettigheter, håndheve programkontroll og sikre tilgang etter minste privilegium til sensitive endepunkter. Administratorer kan tilpasse tilgangsbegrensninger til både endepunkter og programmer. Kontrollene omfatter tillatelses- og sperrelister, kontroll av underprosesser, fjerning av administratorrettigheter på endepunktnivå, just-in-time-tilgang til programmer og rettighetsheving knyttet til bestemte endepunkter.

NIS2-avsnitt	Relevante PAM-kontroller og beste praksis	Hvordan PAM360 hjelper
	- innføre et system for privilegert tilgangsstyring som reduserer risiko ved å overvåke, ta opp, skygge og kontrollere privilegerte sesjoner, og dermed hindre spredning av skadevare.	- Med PAM360s detaljerte programkontroll kan administratorer tillate eller blokkere bestemte programmer på kritiske endepunkter basert på flere sikkerhetsfaktorer. Dette begrenser den mulige angrepsflaten betydelig og gir et ekstra sikkerhetslag for privilegerte sesjoner. Administratorer kan også konfigurere selvbetjent rettighetsheving på programnivå for utvalgte programmer på utvalgte endepunkter eller grupper, slik at brukere kan kjøre godkjente programmer med forhøyede rettigheter i en begrenset periode. - PAM360s modul for sesjonsstyring lar administratorer overvåke, ta opp og arkivere privilegerte sesjoner. Sanntidsovervåkningen bidrar til å oppdage og avslutte mistenkelige brukersesjoner raskt for å redusere risikoen for databrudd. Dette hjelper sikkerhetsteam med å hindre mulig uautorisert bruk av klassifiserte kontoer.

NIS2-avsnitt	Relevante PAM-kontroller og beste praksis	Hvordan PAM360 hjelper
		- Sesjonsopptak og logger er tilgjengelige ved behov for periodiske revisjoner. De gjør det mulig å gå tilbake og kontrollere gamle sesjoner, og de støtter etterlevelse av regulatoriske krav.
85: Sikkerhet i leverandørkjeden	1. Virksomheten bør innføre et system for hemmelighetsstyring med følgende funksjoner: - Et sentralisert hvelv for alle hemmeligheter, slik at man får en samlet oversikt over hemmeligheter som brukes av både mennesker og ikke-menneskelige identiteter. Dette reduserer risiko i leverandørkjeden. - Mulighet til å lagre, rotere, hente nyeste hemmeligheter og bruke dem i både sky- og hybride miljøer.	- PAM360 tilbyr et sentralisert enterprise-hvelv for legitimasjon som samler, lagrer, administrerer og roterer delt sensitiv informasjon, som passord, SSL/TLS-sertifikater, tjenestekontoer, applikasjonskontonøkler og proprietære dokumenter for et bredt spekter av hybride ressurser. - PAM360 hjelper også DevOps-team med å håndtere risikoen ved innebygd legitimasjon gjennom integrasjon med CI/CD-verktøy, RPA-verktøy og containerplattformer. Integrasjonen gjør at prosesser og applikasjoner trygt kan hente hemmeligheter fra PAM360s arkiv og utføre privilegerte operasjoner.

NIS2-avsnitt	Relevante PAM-kontroller og beste praksis	Hvordan PAM360 hjelper
	- Fjernebruk av hardkodet legitimasjon og hemmeligheter i applikasjoner, skript, filer og andre ikke-menneskelige identiteter på tvers av DevOps- og CI/CD-løp. 2. Virksomheten bør innføre en policy for just-in-time privilegert tilgang til utviklingsmiljøer, applikasjoner, databaser osv., inkludert sesjonsopptak og revisjon. Dette reduserer risikoen for angrep via leverandørkjeden.	- Dette kan brukes til å automatisere og orkestrere tilgangstildeling, detaljert kontroll og revisjon uten å forstyrre utviklingsrutinene. 2. Med PAM360 kan dere etablere arbeidsflyter for passordforespørsel og frigivelse. Slike arbeidsflyter krever godkjenning for hver tilgangsforespørsel. Brukere må oppgi årsak til tilgangen, og administratorer blir varslet. Etter verifisering kan administrator velge om tilgang skal gis. Tilgangen kan kombineres med en just-in-time-betingelse som gir tidsbegrenset tilgang. Arbeidsflyten kan også kombineres med app-only tilgangskontroll for å håndheve en mer detaljert praksis for minste privilegium.

NIS2-avsnitt	Relevante PAM-kontroller og beste praksis	Hvordan PAM360 hjelper
		2. Arbeidsflyten kan videre integreres med de fleste større ITSM-verktøy på markedet. Når integrasjonen er aktivert, kan administratorene gi sikker fjerntilgang til målsystemene bare til autoriserte teknikere, uten å dele legitimasjon, ved å validere tilgangsforespørsler mot riktig sak- eller endrings-ID. 3. Med PAM360s funksjoner for endpoint privilege management kan IT-administratorer håndheve tilgangskontroller som er tilpasset endepunkter og applikasjoner. Kontrollene omfatter tillatelses- og sperrelister, kontroll av underprosesser, fjerning av lokale administratorrettigheter, just-in-time-tilgang til programmer og rettighetsheving for bestemte endepunkter.

NIS2-avsnitt	Relevante PAM-kontroller og beste praksis	Hvordan PAM360 hjelper
Artikkel 21, 2(g): Grunnleggende cyberhygiene		
49: Cyberhygienepolicyer for infrastruktur	1. Legitimasjon må lagres i et sikkert, sentralisert hvelv og roteres periodisk i tråd med krav til etterlevelse. 2. Tilgangskontroll må konfigureres for å innføre minste privilegium for privilegerte kontoer i informasjonssystemer. 3. Lokale administratorrettigheter må fjernes på alle endepunkter og erstattes med just-in-time rettighetsheving. 4. Passord for privilegerte kontoer bør sikkerhetskopieres for å kunne reagere effektivt og proaktivt ved cybertrusler eller hendelser.	1. PAM360 gir et sentralisert enterprise-hvelv for legitimasjon, sikret med AES-256-kryptering. Her kan virksomheten samle, lagre, administrere og rotere delt sensitiv informasjon, som passord, digitale sertifikater, nøkler og proprietære dokumenter. Løsningen støtter også masseoperasjoner, for eksempel periodisk passordtilbakestilling, endring og deling for valgte grupper, tilpasset sikkerhets- og etterlevelseskrav. 2. PAM360 innfører prinsippet om minste privilegium gjennom rolle- og policybasert tilgangskontroll, slik at brukere bare får rettighetene de trenger. I tillegg overvåker og tar PAM360 opp privilegerte sesjoner, som gir ansvarlighet og styrker sikkerheten.

NIS2-avsnitt	Relevante PAM-kontroller og beste praksis	Hvordan PAM360 hjelper
		3. PAM360 tilbyr just-in-time rettighetsheving som gir midlertidig tilgang til sensitive servere og arbeidsstasjoner. Dermed kan lokale administratorrettigheter fjernes på sensitive endepunkter, og risikoen for rettighetseskalering reduseres. 4. PAM360 lagrer passord i sitt innebygde legitimasjonsarkiv med sikker passordtilbakestilling og detaljert delingskontroll. Administratorer kan også se hele passordhistorikken for privilegerte kontoer og utløse periodiske passordendringer.

NIS2-avsnitt	Relevante PAM-kontroller og beste praksis	Hvordan PAM360 hjelper
89: Cyberhygiene for brukere	1. Zero Trust-prinsipper bør brukes når det gis tilgang til privilegerte ressurser og privilegerte kontoer som brukes for å nå disse ressursene. 2. Just-in-time tilgang bør aktiveres for brukere som benytter privilegerte kontoer. 3. MFA bør aktiveres for alle brukere som får tilgang til kritiske ressurser. 4. AI og maskinlæring bør brukes til å etablere en risikoscore for brukere. Basert på denne scoren bør tilgang til kritiske ressurser tillates eller nektes.	1. PAM360 lar administratorer håndheve et dynamisk tillitsscoresystem for brukere og enheter. Tillitsscoren beregnes ut fra tilpassbare faktorer dere selv velger. For brukere og endepunkter kan dette for eksempel være antall ugyldige innloggingsforsøk, innlogging utenfor arbeidstid, tillatte IP-adresser, brannmurstatus, OS-versjon, godkjente nettlesertillegg, tjenester og mer. Basert på tillitsscoren kan administratorer opprette og knytte tilgangspolicyer til kritiske endepunkter. Policyene avgjør om en privilegert bruker skal få tilgang til en enhet eller ikke, ut fra nødvendig tillitsscore. Hvis scoren faller, kan policyen automatisk trekke tilbake tilgang. 2. Med PAM360 kan dere gi midlertidig just-in-time tilgang til privilegerte brukere. En arbeidsflyt for forespørsel og frigivelse kombinert med en tidsbetingelse sørger for at en brukers fjernsesjon avsluttes straks den tildelte tiden er ute. Administratorer kan også gi en utsettelsesperiode, og løsningen varsler brukeren før avslutning om hvor mye tid som gjenstår til å fullføre pågående oppgaver. I tillegg til midlertidig tilgang kan dere midlertidig heve rettigheter for en brukerkonto slik at administrative oppgaver kan utføres selv om de ikke er tillatt med brukerens ordinære tilgangsnivå.

NIS2-avsnitt	Relevante PAM-kontroller og beste praksis	Hvordan PAM360 hjelper
89: Cyberhygiene for brukere		3. PAM360 tilbyr flerfaktorautentisering for å styrke sikkerheten. Løsningen støtter flere MFA-metoder, blant annet SMS, e-post, TOTP og tredjeparts autentiseringsapper, og gir et ekstra beskyttelseslag ved tilgang til sensitiv informasjon og kritiske systemer. 4. Administratorer kan også integrere PAM360 med SIEM- og UEBA-verktøy. Dette gir mer avansert korrelasjon av sikkerhetshendelser og bedre beslutningsgrunnlag. Administratorer har full oversikt over hvert privilegert endepunkt og hver bruker, og blir varslet ved uautorisert tilgang. PAM360s tillitsscore profilerer brukere og enheter basert på ulike risikofaktorer. Scorene gir viktig innsikt og kan også brukes til automatiserte handlinger som effektiviserer håndteringen av privilegert tilgang. Basert på samlet tillitsscore kan virksomheter definere minimumsscore for brukere og enheter. Deretter kan egendefinerte policyer utløse automatiske tiltak når score faller under terskel. Dette reduserer behovet for manuell overvåkning og frigjør sikkerhetsadministratorer til viktigere oppgaver.

NIS2-avsnitt	Relevante PAM-kontroller og beste praksis	Hvordan PAM360 hjelper
89: Cyberhygiene for brukere		5. PAM360 gir IT-administratorer detaljert kontroll over endepunktsikkerhet med funksjoner for programkontroll. De kan opprette tillatelseslister for å begrense hvilke programmer brukere kan kjøre, sperrelister for uønskede programmer og kontroll over hvilke programmer som kan startes av godkjente programmer (kontroll av underprosesser). PAM360 gjør det også mulig å fjerne unødvendige lokale administratorrettigheter, gi midlertidig tilgang til bestemte programmer (just-in-time) og konfigurere rettighetsheving basert på individuelle endepunkter. Dere kan også bruke programtillatelseslister og app-only tilgangskontroller for å angi hvilke programmer brukere kan bruke med administratorrettigheter under fjernsesjoner. Denne flerlagstilnærmingen sikrer at brukerne bare får tilgangen de trenger for å utføre oppgavene sine, og reduserer angrepsflaten.

NIS2-avsnitt	Relevante PAM-kontroller og beste praksis	Hvordan PAM360 hjelper
98: Sikring av offentlige elektroniske kommunikasjonsnett	Bruk av sterk kryptering, særlig ende-til-ende-kryptering, og datasentriske sikkerhetsprinsipper som segmentering, merking og tilgangskontroll bør fremmes for å beskytte offentlige elektroniske kommunikasjonsnett og tjenester. I enkelte tilfeller kan kryptering være obligatorisk for å ivareta sikkerhet og innebygd personvern. Medlemsstatene beholder myndighet til å håndheve nasjonal sikkerhet og lovpålagte tiltak, men slike tiltak må ikke svekke styrken eller integriteten til ende-til-ende-kryptering, som er avgjørende for å beskytte data, personvern og sikker kommunikasjon.	For å møte NIS2s krav til ende-til-ende-kryptering og datasentrisk sikkerhet integrerer PAM360 avansert krypteringsteknologi for å beskytte privilegert legitimasjon og hemmeligheter, enten de brukes av mennesker, applikasjoner eller maskiner. Sensitive tilgangsdata forblir kryptert både under overføring og lagring, i tråd med krav til ende-til-ende-kryptering. PAM360 støtter også datasentriske prinsipper som segmentering og håndheving av tilgangspolicyer ved å isolere privilegerte sesjoner og begrense sideveis bevegelse. Det reduserer risikoen for spredning av skadevare i sammenkoblede systemer. Med PAM360 styres tilgang av detaljerte, policybaserte regler for hvem som kan få tilgang til hva, når og under hvilke betingelser. PAM360 automatiserer tilgangsbeslutninger ved hjelp av JIT-rettighetsheving, slik at forhøyet tilgang kun gis når det er nødvendig og i begrenset tid.

NIS2-avsnitt	Relevante PAM-kontroller og beste praksis	Hvordan PAM360 hjelper
Artikkel 21, 2(b): Hendelseshåndtering		
102: Hendelsesrapportering	1. Revisjonsspor og opptak av privilegerte sesjoner bør gi dokumentasjon av cyberhendelser. 2. Det bør finnes en mekanisme for automatisk å identifisere og rapportere avvikende atferd som kjennetegner et sikkerhetsbrudd. 3. Bruk AI og maskinlæring til automatisk å identifisere mistenkelige brukeraktiviteter.	1. PAM360s revisjonsspor registrerer umiddelbart alle hendelser knyttet til privilegerte kontoer og viktige aktiviteter, innloggingsforsøk og planlagte eller fullførte oppgaver. Dataene hjelper virksomheten med interne revisjoner og etterforskning, og viser hvem som fikk tilgang til hvilke ressurser eller filer, hvor, når og hvorfor. 2. Integrasjon mellom PAM360 og tredjeparts SIEM-verktøy gir sanntidskonsolidering og korrelasjon av brukeraktiviteter, ressurser og trusler, slik at skadelige aktører kan identifiseres og isoleres fortløpende. Integrasjonen gir også sikkerhetsteam dypere kontekst og innsikt i hvordan privilegerte kontoer er fordelt, koblet sammen og brukt i organisasjonen. Dette legger et ekstra sikkerhetslag til forsvarsstrategien.

NIS2-avsnitt	Relevante PAM-kontroller og beste praksis	Hvordan PAM360 hjelper
102: Hendelsesrapportering		På denne måten kan IT-team bruke tid og ressurser på å analysere årsaken til sikkerhetshendelser og redusere trusler gjennom nødvendige forebyggende og korrigerende tiltak. 3. PAM360 integreres med ManageEngine Log360 UEBA, som bruker bruker- og enhetsatferdsanalyse (UEBA) til å analysere revisjonslogger og oppdage unormal atferd basert på risikoscore, avvikstrender og revisjonsrapporter. Ved å integrere PAM360 med Log360 UEBA kan hendelsesdata fra PAM360 hentes inn i Log360 UEBA. Revisjonssporene fra PAM360 sendes til Log360 UEBA med jevne mellomrom. Dette gjør det mulig for administratorer å samle og visualisere revisjonsspor for ressurser og brukere, og lage omfattende rapporter. Administratorer kan også overvåke og bygge brede mønstre for brukeratferd, noe som hjelper IT-team med å ta informerte sikkerhetsbeslutninger basert på videre undersøkelser.

NIS2-beredskap: Kom i gang

Mens EU-medlemsstatene ferdigstiller regelverket som implementerer NIS2-direktivet, kan virksomheter ta følgende proaktive steg for
å forberede seg på kravene innen oktober 2024.

- Vurder virksomhetens sikkerhetsstatus

En grundig sikkerhetsrevisjon kan hjelpe IT- og etterlevelsesteam med å avdekke sikkerhetsblindsoner, inkludert risikable feilkonfigurasjoner, for vide rettigheter, utdaterte kontoer, utløpte sertifikater og lignende. Dette gir ledelsen presis informasjon om dagens sikkerhetsnivå, som kan brukes til bedre beslutninger.

- Prioriter privilegert tilgangsstyring

NIS2 anbefaler strenge tiltak for tilgangsstyring for å begrense tilgang til kritiske administratorkontoer. Direktivet fremhever også viktigheten av god cyberhygiene, inkludert PAM, for å hindre at angripere får tilgang til kritisk infrastruktur gjennom feiladministrert legitimasjon.

- Innfør Zero Trust-kontroller

Virksomheter må tenke utover tradisjonelle sikkerhetsarkitekturer og ta i bruk en Zero Trust-tilnærming for å styrke sikkerheten i hybride arbeidsmiljøer. Med Zero Trust kan man legge på flere forsvarslag, som adaptiv autentisering, minste privilegium, trusselanalyse for privilegert tilgang og policy- og rollebasert tilgang for å kontrollere privilegert tilgang.

- Sikre leverandørkjeden

Angrep mot leverandørkjeder er en viktig drivkraft bak NIS2-direktivet. Med økende antall cyberangrep mot programvareleverandørkjeden må virksomheter innføre gode kontroller for hemmelighetsstyring for å beskytte og sikre stabile utviklings- og driftsrutiner.

- Bygg en sikkerhetsorientert kultur

Når menneskelige faktorer er involvert i over 75 prosent av interne angrep, er det avgjørende at virksomheter gir ansatte opplæring og utvikler en kultur for streng cyberhygiene.

Vil du vite hvordan PAM360 kan hjelpe deg med PAM-kravene i NIS2-direktivet?

Kontakt oss

hei@disnova.no
+47 359 74 400

Ansvarsfraskrivelse: Full implementering av NIS2-direktivet krever en rekke prosesser, policyer, mennesker og teknologiske kontroller. Løsningene som er beskrevet her, er begrenset til kontroller for privilegert tilgangsstyring som PAM360 tilbyr for å bidra til etterlevelse av NIS2-krav. Sammen med egnede løsninger, prosesser, menneskelige kontroller og policyer kan ManageEngines PAM360 hjelpe organisasjoner med å tilpasse seg NIS2-direktivet. Dette materialet er kun ment som informasjon og skal ikke anses som juridisk rådgivning om NIS2-etterlevelse. ManageEngine gir ingen garantier, verken uttrykte, underforståtte eller lovpålagte, for informasjonen i dette materialet. Kontakt juridisk rådgiver for å få vite hvordan NIS2-direktivet påvirker organisasjonen og hva dere må gjøre for å etterleve direktivet.