INNOFACTOR | okta

Sjekkliste for din NIS2 Compliance:

7 trinn for forberedelse

Den kommende NIS2-direktivet fra EU introduserer nye forpliktelser for bedrifter for å styrke cybersikkerhet, gjennomføre regelmessige revisjoner og rapportere hendelser raskt. Compliance er obligatorisk for organisasjoner som tilbyr essensielle tjenester - men er også avgjørende for de som konkurrerer om å være deres leverandører. Gjennom solid Identity-håndtering kan organisasjoner kontrollere tilgang, styrke autentisering og etablere ansvarlighet med en lett tilgjengelig revisjonsspor.

Gjør bedriften din klar for NIS2 med disse nøkkelhandlinger.

1. Identifiser dine cybersikkerhetsrisikoer

Sårbarheter kan gjemme seg gjennom nettverket ditt, systemer og eiendeler, og utsette deg for risiko. For eksempel kan uadministrerte passord eller feilkonfigurerte/inaktive kontoer være sårbare for legitimasjonstyveri. Gjennomfør en grundig sikkerhetsvurdering for å finne problemene, vurdere deres påvirkning og begynn å ta skritt for å redusere dem.

- **Kritisk:** Gjennomfør en virksomhetsomfattende risikovurdering og utform en plan for å redusere sårbarheter.

2. Stram opp tilgangskontrollen

Blokkering av uautorisert tilgang til systemer og brukerkontoer er avgjørende for å forhindre datainnbrudd. Gjennomfør streng tilgangskontroll med en solid identitetsplattform som sentraliserer brukeradministrasjon og lar deg definere granulære autorisasjonspolicyer, slik at bare autoriserte personer kan få tilgang til spesifikke ressurser eller utføre visse handlinger.

- **Kritisk:** Implementer solid Identity-governance for å håndheve strengere tilgangskontroll.

INNOFACTOR | okta

3. Beskytt privilegert tilgang

Angripere kan utnytte privilegerte kontoer for å orkestrere angrep, ta ned kritisk infrastruktur og forstyrre essensielle tjenester. Beskytt privilegert tilgang ved å begrense tilgangen til administratornivåkontoer og regelmessig rotere administrative passord.

- **Kritisk: Beskytt privilegerte kontoer med beste praksis, for eksempel minst privilegiumtilgang.**

4. Implementer MFA mot phishing

Med økende sosiale ingeniørangrep krever NIS2 at organisasjoner implementerer MFA mot phishing. Dette gir en ekstra sikkerhetslag ved autentisering av ansatte, kunder og entreprenører, uten å legge til friksjon i deres digitale opplevelse.

- **Kritisk: Rull ut MFA mot phishing for å styrke autentiseringen uten å legge til friksjon.**

5. Styrk forsvarsverket mot ransomware

Kostbare og lamslående ransomware-angrep er en av hoveddriverne for NIS2. Introduser sikkerhetsløsninger for å proaktivt forsvare mot dem, for eksempel endpoint privilege management for å håndheve prinsippet om minst privilegium, kontrollere applikasjoner og styrke neste generasjons antivirus- og løsninger for respons på endepunkter.

- **Kritisk: Introduser sikkerhetsløsninger for å proaktivt forsvare mot ransomware, for eksempel endpoint privilege management.**

INNOFACTOR | okta

6. Gjennomgå din programvareleverandørkjede

Den programvaren du bruker fra tredjepartsleverandører kan være infisert med skadelig kode. Ta en grundig titt på din programvareleverandørkjede og vurder å implementere en løsning for håndtering av hemmeligheter for å trygt lagre sensitiv informasjon, som passord, nøkler og token.

- **Kritisk:** Vurder å implementere en løsning for håndtering av hemmeligheter for å redusere risikoen for angrep mot forsyningskjeden.

7. Gå over til en Zero Trust-strategi

Tradisjonelle sikkerhetsarkitekturer basert på perimetre er ikke egnet for dagens grenseløse verden av skytjenester og hybride arbeidsstyrker. Vurder å gå over til en flernivå Zero Trust-tilnærming, drevet av robust identitetsadministrasjon, som håndhever minst privilegium-tilgang, kontinuerlig autentisering og trusselanalyse.

- **Kritisk:** Ta i bruk en Identity-drevet Zero Trust-strategi som gir riktig tilgang, til riktige ressurser, til riktig tid.

Kilde: Okta NIS2 Compliance Checklist

INNOFACTOR | okta