Checklist inzake NIS2-naleving

bechtle

veeam

Bent u er achter gekomen dat u moet voldoen aan de NIS2-richtlijn? Er achter komen welke stappen u moet nemen om compliant te zijn, is niet iets wat u de ene op de andere dag weet en regelt. We hebben deze handige checklist opgesteld, zodat u hiervoor een plan van aanpak kunt opstellen. De sancties voor het niet naleven kunnen verstrekkende gevolgen hebben, dus zorg ervoor dat u weet wat er op het spel staat, voor u persoonlijk en voor uw organisatie. We richten ons met name op artikel 21 en 23, waarin de nalevingsverplichtingen worden beschreven. Ga naar onze website voor meer informatie over NIS2 en de mogelijke gevolgen voor uw bedrijf.

Artikel over NIS2	Vraag het uzelf af...	Hoe het Veeam Data Platform kan helpen
21-2(a): beleid ten aanzien van risicoanalyse en beveiliging van informatiesystemen;	◯ Weet ik welke risico's ik in mijn huidige omgeving loop? ◯ Heb ik inzicht in interne- en externe factoren? ◯ Kan ik als het noodlot toeslaat binnen de afgesproken hersteltijd herstellen?	**Foundation:** Ingebouwde beveiliging en controle op naleving **Advanced:** Rapporten over afwijkingen en trends **Premium:** Dagelijkse rapporten over gereedheid
21-2(c): bedrijfscontinuïteit, zoals back-upbeheer, disaster recovery en crisisbeheer;	◯ Heb ik back-ups van alle belangrijke systemen? ◯ Ik heb workloads naar de cloud verplaatst. Zijn ze daar veilig? ◯ Kan ik zonder extra resources snel herstellen na de uitval van systemen? ◯ Hebben we beleid inzake cyberhygiëne?	**Foundation:** Tags zorgen ervoor dat er van nieuwe workloads back-ups worden gemaakt **Advanced:** Altijd en overal volledig overzicht van uw workloads **Premium:** Herstellen naar Azure als uw reserve-datacenter
21-2(i): personeelsbeveiliging, toegangsbeheerbeleid en beheer van middelen;	◯ Kan ik niet-geautoriseerde gebruikers weren? ◯ Maak ik nog steeds gebruik van onveilige wachtwoorden? ◯ Kan een kwaadwillende beheerder mijn herstelopties manipuleren? ◯ Heb ik al het personeel zodanig opgeleid dat zij weten hoe ze veilig moeten omgaan met gegevens?	**Multifactor-authenticatie** en op rollen gebaseerd toegangsbeheer Ondersteuning voor **belangrijke externe beheersystemen** Immutable opslaglocaties, zowel **on-premises als in de cloud**
23-4(a) en (b): Maak melding van een incident bij het computerincident bestrijdingsteam (...) zonder onnodige vertragingen en in elk geval binnen 24(a)/72(b) uur nadat u zich bewust bent geworden van het significante incident,	◯ Hoe weet ik welke systemen in een noodsituatie getroffen zijn? ◯ Hoe gaan we om met kwetsbaarheden en openbaarmaking daarvan? ◯ Hoe maak ik melding van incidenten aan het computerincident bestrijdingsteam? ◯ Kan ik deadlines voor rapporten halen als mijn systemen niet werken?	**Ingebouwde malware-** en **YARA-scans op regels** om aangetaste systemen te identificeren **Vooraf geconfigureerde rapporten** klaar om in te dienen bij het **Best practices** om de beschikbaarheid van Veeam-rapporten te garanderen

Vul de hiaten in uw cyberbeveiliging met Veeam

Bevindt u zich niet in de EU en denkt u dat u bent vrijgesteld? Vervelend nieuws, dat bent u niet...
NIS2 is van invloed op toeleveringsketens en heeft verstrekkende invloed. Neem vandaag nog contact met ons op en ontdek hoe we u kunnen helpen om nu een begin te maken met uw nalevingstraject.

LATEN WE PRATEN

* Let op: dit rapport is slechts een voorbeeld en we raden u aan juridisch advies in te winnen over uw specifieke verplichtingen ten aanzien van NIS2-naleving