AON

Bestuurders, kom in actie

NIS2 vraagt om cultuurverandering

NIS2 is er voor u het weet. De nieuwe cyberwetgeving op basis van de EU-richtlijn zal al vanaf eind 2024 gevolgen hebben voor veel organisaties en tegelijkertijd ook kansen bieden. Meer organisaties dan voorheen zullen worden aangemerkt als ‘belangrijk’ of ‘essentieel’ en te maken krijgen met wettelijke verplichtingen. NIS2 vraagt om de volledige focus op het goed inrichten van cybersecurity.

Veel organisaties zullen dit zien als het puur afvinken van verplichtingen; maar daarmee slaan ze de plank mis. Het biedt namelijk ook de kans om serieus werk te maken van een organisatiecultuur waarin cybersecurity in alle lagen is verankerd. Dit stelt organisaties in staat zich als vertrouwde partner te profileren, investeringen aan te trekken en hun concurrentiepositie te vergroten. Maar een succesvolle, effectieve implementatie van NIS2 is afhankelijk van hoe organisaties hun cyberstrategie aanpassen en hierover naar iedereen communiceren. Dit doe je er niet even bij; het vraagt om een cultuurverandering.

Wat verandert er precies?

De Network and Information Security directive (NIS2) is veeleisender dan de huidige cyberwet en komt met strengere maatregelen. De richtlijn heeft tot doel het:

- versterken van capaciteiten op het gebied van cyberbeveiliging binnen de hele EU;
- beperken van kwetsbaarheden in het netwerk en in de informatiesystemen die zijn gebruikt binnen essentiële en belangrijke sectoren;
- waarborgen van de continuïteit van deze organisaties wanneer zij zijn aangevallen en een cyberincident het gevolg is.

Wat is het risico?

Het risico bestaat dat organisaties de nieuwe wetgeving hetzelfde benaderen als bijvoorbeeld de introductie van de AVG enige jaren geleden. Daar werd twee jaar voor uitgetrokken. In 2016 zei men: ‘Dat komt wel, en met die boetes zal het ook zo’n vaart niet lopen’. Door die instelling begon het naleven van de privacywetgeving pas in 2020 echt te leven. Dit dreigt weer te gebeuren, vooral omdat bestuurders niet precies weten wat hen te wachten staat. Er is nog veel onbekendheid met het onderwerp, laat staan dat de organisatie erop ingericht is om te voldoen aan de eisen vanuit NIS2. Anders dan bij de privacywetgeving echter kunnen bestuurders nu persoonlijk aansprakelijk gesteld worden voor het niet nakomen van hun verplichtingen. Dit geldt zelfs voor de CISO binnen de organisatie, mits deze de relevante bevoegdheden en verantwoordelijkheden heeft. Dit gaat dus een stuk verder dan de boetes bij de privacywetgeving.

Wat betekent dit voor bestuurders?

De nieuwe wetgeving brengt (aansprakelijkheids)risico’s met zich mee. Om deze het hoofd te kunnen bieden, is een cultuurverandering binnen organisaties nodig, een andere mindset. Het belang van cybersecurity moet tot in de haarvaten van de organisatie zijn doorgedrongen. Daarbij is het de taak van het bestuur om uit te dragen dat cyberrisico’s de hoogste prioriteit hebben. Als de ‘tone at the top’ niet verandert, gaat deze boodschap nooit landen bij managers en medewerkers. Een organisatie die deze benodigde cultuurverandering heeft doorgemaakt, kenmerkt zich als volgt:

De kenmerken van een NIS2-cyberveilige organisatie

- Er wordt door het bestuur duidelijk gecommuniceerd wat de visie en waarden zijn die horen bij NIS2. Managers en medewerkers begrijpen deze communicatie en voeren de benodigde veranderingen door in de organisatie.
- Cybersecurity is als onderdeel in de organisatiestrategie opgenomen en toont hiermee aan dat de organisatie weerbaarder wil zijn tegen cyberaanvallen.
- Het bestuur vertoont het gewenste gedrag om de veranderingen binnen de cultuur van de organisatie uit te dragen naar iedereen. Medewerkers accepteren de veranderingen als zij zien dat het bestuur en de managers dit ook doen.
- De mindset, vaardigheden en gewoonten van iedereen binnen de organisatie worden op peil gehouden door training en ontwikkeling. Iedereen is ervan doordrongen dat elke organisatie vatbaar is voor een cyberaanval.
- De cultuurverandering wordt geëvalueerd zodat problemen aan de bestuurstafel besproken worden en veranderingen kunnen worden doorgevoerd. Het bestuur luistert naar de dynamiek van de organisatie, optimaliseert waar nodig en past de effectiviteit naar aanleiding van ontvangen feedback.
- Het bestuur is zich ervan bewust dat cultuurveranderingen tijd kosten en is vasthoudend aan haar visie om cybersecurity binnen de organisatie te verbeteren, ook als het even niet mee zit.

Zet als bestuur een cultuurverandering in gang

Om er als bestuur voor te zorgen dat het cyberbeleid in de haarvaten van de organisatie doordringt, zal het een cultuurverandering in gang moeten zetten. Dat betekent luisteren naar de organisatie, kennis opdoen, trainen, het beleid actief in de organisatie communiceren en zelf het goede voorbeeld geven. Door deze veranderingen mee te nemen in de organisatie zal de cultuur langzaam verbeteren in de houding naar cybersecurity. Dit kost tijd, dus gebruik de tijd die u heeft en begin vandaag.

In 10 stappen naar een nieuwe cyberveilige organisatiecultuur

Wilt u weten welke stappen er nodig zijn voor het verankeren van NIS2 cyberveiligheid in uw organisatie?

Lees het hier

Contact

Frank Ruijgrok
Principal Consultant Aon Cyber Solutions
frank.ruijgrok@aon.nl
+31 6 4612 3988

aon.nl/nis2

Over Aon

Aon plc (NYSE: AON) zet zich in voor betere besluitvorming — om mensen over de hele wereld te beschermen en hun bestaan te verrijken. Onze medewerkers leveren advies en oplossingen die onze klanten in meer dan 120 landen en soevereiniteiten duidelijkheid en vertrouwen geven om betere beslissingen te nemen waarmee zij hun bedrijf beschermen en laten groeien.

Volg Aon op on LinkedIn, X, Facebook en Instagram. Blijf op de hoogte door Aon's Newsroom te bezoeken en meld je hier aan voor News Alerts.