WHITEPAPER

Zo wordt jouw ICT-omgeving NIS2-ready

avit
part of springboardnetwork

Veel organisaties krijgen in de zomer van 2024 te maken met de vanuit de EU opgelegde NIS2-wetgeving. Deze security-richtlijnen moeten de digitale weerbaarheid van Europa verbeteren. Organisaties die niet voldoen aan de wet riskeren hoge boetes. Hou hier de tijdlijn in de gaten. Om niet onaangenaam te worden verrast, is het belangrijk om jouw organisatie op tijd voor te bereiden op NIS2. Avit kan je helpen om jouw ICT-omgeving NIS2-ready te maken. In dit whitepaper lees je hoe wij adviseren en ondersteunen.

In dit whitepaper lees je hoe Avit ondersteunt met:

- ✓ Veilige netwerk- en informatiesystemen
- ✓ Basismaatregelen voor cyberhygiëne (die elke organisatie minimaal moet nemen)
- ✓ Een veilig communicatiesysteem én noodoplossing

VOOR WIE GELDEN DE NIS2-RICHTLIJNEN?

NIS2 is een vervolg op de bestaande NIS-wet, die alleen van toepassing is op zes kritieke sectoren: financiën, energie, water, zorg, transport en digitale infrastructuur. NIS2 gaat voor veel meer organisaties gelden: minimaal zeventien. De richtlijn geldt niet alleen voor overheidsinstanties en essentiële bedrijven, maar ook voor belangrijke organisaties zoals postbezorging, fabrikanten van medische hulpmiddelen en bedrijven in de voedselindustrie. Deze sectoren zijn door de EU bepaald. De Nederlandse overheid heeft de vrijheid om nog meer sectoren toe te voegen die aan NIS2 moeten voldoen; bijvoorbeeld omdat ze belangrijk zijn voor de Nederlandse samenleving.

Wat gebeurt er als je de regels niet naleeft?
Zoals gezegd gaat de Nederlandse NIS2-wet in juli 2024 in. Het niet naleven van de richtlijnen kan organisaties op forse boetes komen te staan: tien miljoen euro voor essentiële organisaties (of 2% van de jaaromzet) en zeven miljoen voor belangrijke bedrijven (of 1,4% van de jaaromzet). De wet zal onder meer gehandhaafd worden met steekproef-controles, audits, scans en aanvragen voor informatie. Daarnaast is de directie van een organisatie niet alleen persoonlijk verantwoordelijk, maar kan zelfs ook persoonlijk aansprakelijk worden gesteld als er een incident plaatsvindt.

Om die reden is het belangrijk om tijdig op een rij te zetten hoe jouw organisatie ervoor staat als het om NIS2 gaat, en advies te vragen waar dat nodig is. Een IT-specialist kan adviseren over de technische invulling van NIS2. Hieronder staat op een rij met welke NIS2-richtlijnen Avit kan assisteren.

ZORG VOOR VEILIGE NETWERK- EN INFORMATIESYSTEMEN

NIS2 schrijft voor dat de security altijd op orde moet zijn als netwerk- en informatiesystemen worden aangeschaft, ontwikkeld en onderhouden. Dat betekent dat netwerkapparatuur niet alleen aan functionele eisen, maar ook aan moderne veiligheidseisen moet voldoen. Het is dan echter wel van belang om te weten wat deze veiligheidsvereisten precies zijn.

Zorg voor de juiste instellingen

Bij het inrichten van apparatuur is vaak veel meer te configureren en open te stellen dan veilig is. Daarom is het belangrijk om een partner in de arm te nemen die op de hoogte is van de juiste veiligheidsinstellingen, zodat alles volgens NIS2-richtlijnen wordt geconfigureerd. Avit kan daar als ervaren netwerkspecialist in ondersteunen.

Hou je systemen up-to-date

Naast de veiligheidsinstellingen bij de inrichting, schrijft NIS2 ook voor dat apparatuur up-to-date gehouden moeten worden. Een netwerk kan bij aanschaf en inrichting best voldoen aan de veiligheidsstandaarden van die tijd, maar is dat na vijf jaar nog steeds het geval? Denk bijvoorbeeld aan het beheer, de manier waarop gegevens worden versleuteld, of de wijze waarop met externe partijen wordt verbonden.

Wellicht wordt al heel lang met een oude software-versie gewerkt, terwijl de nieuwe versie veel beter en veiliger is. Een netwerk- en security-specialist kan zorgen dat systemen up-to-date blijven, zodat ze altijd aan de laatste veiligheidseisen (en dus NIS2) voldoen.

Blijf monitoren en dicht gaten

Naast het veilig inrichten en up-to-date houden van jouw apparatuur, is het ook belangrijk om het systeem te monitoren op kwetsbaarheden. Succesvolle cyber-aanvallen vinden vaak plaats door bekende kwetsbaarheden die nooit zijn verholpen. Dat is te voorkomen door een ervaren partij, zoals Avit, jouw systeem regelmatig te laten controleren. Zo worden gaten op tijd gedicht.

“Het is belangrijk om een partner in de arm te nemen die op de hoogte is van de juiste veiligheidsinstellingen”

VOLDOEN AAN DE BASISREGELS VOOR CYBERHYGIËNE

NIS2 schrijft daarnaast voor dat organisaties moeten zorgen voor goede cyber-hygiëne. Daarbij wordt gedoeld op 56 maatregelen, opgesteld door het Center for Internet Security, die ervoor zorgen dat jouw systemen in de basis veilig zijn. Bekende technische onderdelen op de lijst zijn bijvoorbeeld multifactor-authenticatie, DNS-filtering, anti-malware en het verzamelen van log-gegevens vanuit applicaties. Avit biedt diensten en oplossingen die ervoor zorgen dat deze onderdelen zijn afgedekt. Zo kan onze SOC-oplossing helpen bij het opvolgen van security-incidenten, één van de verplichtingen van NIS2.

Peil je weerbaarheid

Dankzij het resilience assessment van Avit kan jouw organisatie samen met een security-expert alle punten van de cyber hygiene-lijst langsgaan. We brengen in kaart in hoeverre jouw organisatie eraan voldoet: zijn de zaken die NIS2 eist op orde? Technische onderdelen kan Avit oplossen. Denk bijvoorbeeld aan het instellen van veilige authenticatie voor remote werken, of het verzamelen van log-gegevens uit software. Bij andere onderdelen kunnen we adviseren om er beleid en procedures voor op te stellen. Het is waardevol om door middel van dit resilience assessment in kaart te brengen wat het volwassenheidsniveau van jouw security is.

RICHT EEN BEVEILIGD COMMUNICATIESYSTEEM ÉN EEN NOODOPLOSSING IN

NIS2 schrijft ook voor dat organisaties altijd gebruik moeten maken van een beveiligd communicatieysteem, voorzien van multifactor-authenticatie. Avit biedt deze oplossingen aan in de vorm van Microsoft Teams en Cisco Webex, waarmee volledig secure kan worden gecommuniceerd via video, audio of chat.

Zet een noodsysteem op

Daarnaast staat in de NIS2-wet omschreven dat er een beveiligd noodsysteem aanwezig moet zijn, waar medewerkers terechtkunnen als er iets mis is met het primaire systeem. Dat betekent dat zo'n noodsysteem bijvoorbeeld niet via Microsoft Teams kan draaien. Het noodsysteem zal dan immers niet werken als er problemen zijn met Teams.

Avit biedt met Cisco Webex een alternatief, veilig communicatiesysteem aan. Omdat dit systeem afzonderlijk van het primaire communicatiesysteem werkt, kunnen medewerkers bij calamiteiten met één druk op de knop blijven communiceren.

Dat werkt natuurlijk ook andersom: wanneer primair met Cisco Webex wordt gewerkt, zal Teams de noodoplossing zijn. Zo'n communicatiesysteem voor noodgevallen is belangrijk voor directe collega's en om snel in contact te treden met betrokken partners.

AVIT ADVISEERT EN ONDERSTEUNT BIJ DE TECHNISCHE INVULLING VAN NIS2

Maak jouw ICT-omgeving NIS2-ready door rekening te houden met bovenstaande onderdelen. Behalve de technische kant, omvat de wet allerlei richtlijnen voor een gedegen security-beleid: denk bijvoorbeeld aan een meldplicht bij incidenten en andere rapportage-vereisten.

Avit kan adviseren en ondersteunen bij de technische invulling van NIS2, maar het is daarnaast van belang om het beleid binnen jouw organisatie onder de loep te nemen. Laat je niet verrassen en zorg dat je vroeg op de hoogte bent van de implicaties van NIS2.

MEER INFORMATIE?

Kijk op www.avitgroup.com of neem contact op:

avit
part of springboardnetwork

T: +31 (0)88 032 10 32
E: info@avitgroup.com