NIS2 risicofactoren

Het doelvan NIS2is dat burgersnietgeraakt worden door cyberincidenten en dat onze economie wordt beschermd. De bedrijven in de NIS2 sectoren maken zelf een afweging over de risico's die zij lopen. Cruciale elementen hierbij zijn:

- **Risicoanalyse:** Bedrijven in de NIS2 sectoren dienen passende en evenredige beveiligingsmaatregelen vast te stellen op basis van een risicoanalyse. Ze moeten inzicht verkrijgen in hun kritieke processen om te bepalen wat de juiste maatregelen zijn, en de maatschappelijke en economische impact van mogelijke incidenten overwegen bij deze risicobeoordeling.
- **All hazards approach:** Bij het beoordelen van risico's moeten organisaties alle bedreigingen voor hun netwerk- en informatiesystemen in ogenschouw nemen, inclusief fysieke gevaren zoals brand, overstroming, diefstal en misbruik. Deze brede 'all hazards approach' strekt zich vaak uit voorbij de directe leverancier of dienstverlener.
- **Gehele toeleveringsketen:** Het is essentieel dat organisaties solide afspraken maken met hun directe toeleveranciers over het implementeren van cyberbeveiligingsmaatregelen. Hierbij kunnen ook overeenkomsten worden gesloten die effecten hebben op subleveranciers.

Geen water uit de kraan

Geen operaties

Haven valt stil

Geen geld uit de muur

Geen verwarming

Lege supermarktschappen

Ramp met chemische stoffen

NIS2 sectoren

Drinkwater | Transport | Bankwezen | Infrastructuur financiële markt | Gezondheidszorg | Energie | Digitale infrastructuur | Beheerders van ICT-diensten | Afvalwater | Overheidsdiensten | Ruimtevaart | Digitale aanbieders | Post- en koeriersdiensten | Afvalstoffenbeheer | Levensmiddelen | Chemische stoffen | Onderzoek | Vervaardiging | Onderwijs

Risico's in de keten

Groter risico

MSP

Een grote MSP die IT-beheerdiensten levert wordt gehackt. Hierdoor is er een direct risico voor de bedrijfsvoering, aangezien de MSP toegang heeft tot kritieke systemen en netwerken. Dit kan leiden tot gegevensdiefstal, verstoring van de dienstverlening en mogelijk lange hersteltijden, waardoor het bedrijf kwetsbaar wordt voor verdere aanvallen.

Service Provider

Na een cyberaanval op een leverancier van pinterminals, worden uit voorzorg alle terminals geblokkeerd. Een bedrijf dat afhankelijk is van fysieke klanttransacties, kan geen elektronische betalingen meer accepteren. Dit kan resulteren in omzetverlies en het vertrouwen van klanten schaden doordat alternatieve betalingsmethoden noodzakelijk zijn.

Telecomprovider

Een grote storing bij een telecomprovider door een cyberaanval kan ertoe leiden dat het bedrijf niet bereikbaar is via internet of telefoon. Dit beïnvloedt alle aspecten van de bedrijfsvoering, van klantcommunicatie tot remote toegang van werknemers, wat resulteert in operationele vertragingen en potentieel verlies van zakelijke mogelijkheden.

ERP systeemleverancier

Een cyberaanval op een ERP-systeemleverancier resulteert in corrupte data en systeemuitval. Een bedrijf dat afhankelijk is van dit systeem voor dagelijkse operaties zoals voorraadbeheer, facturatie en inkoop, staat stil. Dit verstoort niet alleen de interne operaties, maar beïnvloedt ook de levering van diensten of producten aan klanten.

Datacenter

Een overstroming in een datacenter waar bedrijfskritische servers en applicaties gehost worden, veroorzaakt aanzienlijke downtime. Als gevolg daarvan kan het bedrijf geen orders verwerken, geen toegang krijgen tot essentiële data en klantenservices zijn offline, wat leidt tot financiële verliezen en imagoschade.

Cloudopslagprovider

Stel dat een cloudopslagprovider die bedrijfsdata opslaat te maken krijgt met een datalek door een ongeautoriseerde toegang. Gevoelige informatie, waaronder intellectueel eigendom en persoonsgegevens, wordt blootgesteld. Dit kan leiden tot juridische gevolgen en het verlies van klantvertrouwen.

Grondstoffenleverancier

Een cyberaanval op een leverancier van essentiële chemicaliën voor de farmaceutische industrie, resulteert de productie van medicijnen, betekent dit een directe verstoring in de toevoer. Wat leidt tot tekorten aan kritieke medicijnen op de markt en potentiële gezondheidsrisico's voor burgers.

Aanval op container terminal

In de zomer van 2017 legde een cyberaanval op een containerterminal in de Rotterdamse haven het transport stil. Duizenden containers konden niet worden verscheept. Schepen en vrachtwagens moesten uitwijken, met flinke vertragingen als gevolg. Deze ketenaanval, die miljoenen aan schade veroorzaakte, had waarschijnlijk niet eens de haven als direct doelwit, maar toont aan hoe breed de impact van een cyberaanval kan zijn.

HVAC Installateurs

Een zorginstelling ondervindt ernstige problemen als hun HVAC-systemen uitvallen door een hack bij de onderhoudsleverancier. Dit zorgt voor een niet-gecontroleerd klimaat waardoor er een verhoogd risico op infecties ontstaat, vooral in kritieke afdelingen zoals operatiekamers en IC's.

Halffabrikaatleverancier

Een ransomware-aanval op een leverancier van halffabrikaten in de bouwsector verstoort de verzendingsprocessen. Dit leidt tot vertragingen in bouwprojecten, waardoor bouwbedrijven hun deadlines missen en contractuele boetes riskeren.

Saas leverancier

Een hack bij een SaaS-leverancier leidt ertoe dat duizenden bedrijven geen toegang meer hebben tot hun klantgegevens. Daardoor zijn sales- en supportteams niet in staat klantinformatie op te roepen, wat resulteert in verstoorde klantrelaties en mogelijk verlies van belangrijke contracten.

Chemicaliënopslag

Een cyberhack op de transportsystemen van een chemische opslagplaats maakt de locatie van gevaarlijke stoffen onduidelijk. Dit resulteert in ernstige veiligheidsrisico's en potentieel gevaarlijke situaties tijdens het hanteren of verplaatsen van deze stoffen.

Machineleverancier

Een belangrijke machineleverancier wordt gehackt, wat resulteert in vertragingen bij de vervanging van cruciale onderdelen voor productielijnen. Dit heeft direct invloed op productiebedrijven, waardoor zij hun productie moeten verminderen of zelfs stilleggen.

Gezondheidszorgdienstverlener

Een systeemfout bij een elektronisch patiëntendossiersysteem in een ziekenhuis door een softwarefout veroorzaakt onjuiste medicatiedoseringen. Dit leidt tot patiëntrisico's en juridische gevolgen voor de zorginstelling.

Bankwezen

Een lokale bank ondervindt een DDoS-aanval, waardoor online bankierdiensten tijdelijk niet beschikbaar zijn. Klanten kunnen geen transacties uitvoeren, wat leidt tot frustraties en een verlies van vertrouwen in de bank.

Digitale provider

Een aanbieder van digitale infrastructuurdiensten ervaart een datalek en daardoor liggen op gebruikersgegevens op straat. Bedrijven die afhankelijk zijn van deze provider moeten snel reageren om maatregelen te treffen om verdere schade te beperken.

Freight broker

Een ransomware-aanval legt de operaties van een freight broker plat, wat leidt tot ernstige vertragingen in de transportsector. Dit veroorzaakt kettingreacties in kostenstijgingen en leveringsvertragingen over diverse industrieën heen.

Onderzoeksinstituut

Een onderzoeksinstituut gespecialiseerd in biotechnologie wordt gehackt, waardoor onderzoeksdata corrupt raakt. Dit stagneert belangrijk onderzoek naar nieuwe geneesmiddelen, resulterend in financiële schade en vertragingen.

Voedselverwerker

Hackers versleutelen de productiedata van een voedselverwerker, waardoor de productielijnen stil komen te liggen. Dit veroorzaakt voedseltekorten en aanzienlijke financiële schade door gemiste omzet en spoedbestellingen bij alternatieve leveranciers.

Installateur

De planning- en communicatietools van een installatiebedrijf worden gecompromitteerd door een cyberaanval. Dit leidt tot een chaotische werkschema, miscommunicatie met klanten, en vertragingen in de uitvoering van projecten, wat klanttevredenheid en inkomsten schaadt.

Distributeur

Een distributeur in de voedselindustrie wordt getroffen door malware, wat leidt tot logistieke verstoringen. Koelsystemen falen en leveringsschema's raken in de war, resulterend in het bederven van versproducten en significante financiële verliezen door afgeschreven voorraad.

Architectenbureau

Bij een architectenbureau dat een ziekenhuis ontwerpt, leidt een datalek tot het verlies van een half jaar aan werk door slecht backupbeleid. De bouw van het ziekenhuis loopt ernstige vertraging op, met financiële en maatschappelijke consequenties.

Verhuurder bedrijfspanden

Een ransomware-aanval treft een verhuurder van bedrijfspanden, waardoor de systemen voor fysieke beveiliging uitvallen. Dit leidt tot ongeautoriseerde toegangen en veiligheidsrisico's voor alle huurders.

De kaashack

In april 2021 werd een belangrijke kaasleverancier van Albert Heijn getroffen door een ransomware-aanval. Dit incident blokkeerde de toegang tot de logistieke systemen van het bedrijf. Ondanks dat de kaasproductie doorging, kon de leverancier de kaas niet distribueren. Als resultaat daarvan was er aanzienlijk minder kaas beschikbaar in de schappen van Albert Heijn.

Personeelsleverancier

Een cyberaanval resulteert in het lekken van het personeelsbestand van een leverancier die beveiligingspersoneel levert aan banken. Dit leidt tot bezorgdheid binnen het bankwezen over de mogelijke chanteerbaarheid van hun beveiligingspersoneel.

Wetenschapscollectief

Onderzoekers van een wetenschapscollectief geven door een phishingaanval vertrouwelijke persoonlijke en projectinformatie prijs. Dit compromitteert belangrijke onderzoeksprojecten en leidt tot ernstige privacy- en veiligheidsproblemen.

Clearing house

Een phishingaanval legt een clearing house enkele uren stil, waardoor de verwerking van financiële transacties op de aandelenmarkt wordt onderbroken. Dit beïnvloedt direct de beurskoersen en kan leiden tot aanzienlijke financiële verliezen voor investeerders.

Leverancier onderdelen

Hackers infiltreren het systeem voor kwaliteitscontrole. Dit resulteert in de productie en levering van defecte onderdelen aan autofabrikanten met alle gevolgen van dien.

Transportbedrijf

Een transportbedrijf ervaart een gijzeling van zijn rittenadministratie. Digitale tachografen functioneren niet meer correct, wat leidt tot grote logistieke verstoringen en financiële verliezen door niet-naleving van leveringsschema's.

Leverancier deuren

Door een hack falen de automatische deuren van operatiezalen in een ziekenhuis. Dit vertraagt spoedeisende operaties, wat kritieke vertragingen voor patiëntenzorg veroorzaakt en kan leiden tot medische complicaties of zelfs levensbedreigende situaties.

Marketing bureau

Een marketingbureau wordt getroffen door een wormvirus dat zich via e-mailbijlagen verspreidt. Ook de systemen van meerdere cliënten worden geïnfecteerd. Dit veroorzaakt niet alleen operationele verstoringen maar ook ernstige reputatieschade voor het bureau en zijn cliënten.

Hack op wasserij

Moderne wasserijen zijn volledig geautomatiseerd. Ook het desinfectieproces wordt digitaal aangestuurd. Door een hack krijgt het ziekenhuis geen gedesinfecteerde lakens meer, waardoor het zorgproces stilvalt - mogelijk zelfs operaties.

Financieel adviseur

Een cyberaanval legt een financieel adviseur tijdelijk stil. Als gevolg hiervan kunnen belangrijke belastingaangiften voor vele klanten niet op tijd worden ingediend, wat leidt tot boetes en financiële complicaties voor de betrokkenen.

Electronica fabrikant

Een phishingaanval bij een fabrikant van elektronica compromitteert de productiegegevens. Dit veroorzaakt fouten in de productieprocessen, wat leidt tot defecte producten die teruggeroepen moeten worden.

Apotheek

Een hack bij een apotheek veroorzaakt een tekort aan kritieke componenten voor medicijnen. Dit heeft directe gevolgen voor patiënten die afhankelijk zijn van dagelijkse medicatie, waardoor hun gezondheid en welzijn in gevaar komen.

Verpakkingsleverancier

Een cyberincident leidt ertoe dat een verpakkingsleverancier zijn productie moet staken. Dit heeft zorgt voor productiestilstanden en leveringsachterstanden bij bedrijven in de voedingsmiddelen- en farmaceutische industrie.

Aannemer

Een aannemersbedrijf heeft een hack in het salarisadministratiesysteem, waardoor werknemers niet betaald kunnen worden. Dit resulteert in een stopzetting van bouwprojecten, vertragingen in de oplevering, en mogelijke juridische geschillen.

Voedselcontroleur

Een cyberaanval manipuleert de veiligheidstests van een voedselcontroleur, waardoor onveilige producten de markt bereiken. Dit resulteert in ernstige gezondheidsrisico's voor consumenten, omvangrijke productterugroepingen, en aanzienlijke reputatieschade voor de producenten.

Accountant

Een cyberaanval op een accountantskantoor leidt tot het compromitteren van financiële gegevens van meerdere cliënten. Dit veroorzaakt vertragingen in de salarisuitbetaling en belastingaangiften, wat financiële stress en mogelijke boetes voor de betrokken bedrijven en hun werknemers veroorzaakt.

Loodgietersbedri

Na een cyberaanval worden alle computers en cloudsystemen gewist bij een loodgietersbedrijf dat verantwoordelijk is voor de water- en verwarmingsinstallaties in diverse woningen en kantoren. Dit resulteert in het uitvallen van essentiële diensten zoals verwarming en watervoorziening, met grote overlast voor burgers en bedrijven als gevolg.

Kleiner risico

Risico analyse

In artikel 21.2d van de NIS2-richtlijn staat dat bedrijven zorgplichtmaatregelen moeten nemen om hun toeleveringsketens te beveiligen. Dit omvat het beveiligen van alle aspecten die betrekking hebben op de relaties tussen een organisatie en haar directe leveranciers en dienstverleners. Belangrijke vragen daarbij zijn:

- Hoe afhankelijk ben je van deze leverancier(s)?
- In welke mate werk je digitaal met deze leverancier(s) samen?

In de ketenrisico-analyse onderscheiden we drie niveaus, waarbij niet elke leverancier dezelfde impact heeft op de bedrijfscontinuïteit bij incidenten. Elk bedrijf dat onder de NIS2-regulering valt, dient zelf de risico's in kaart te brengen die specifieke leveranciers met zich meebrengen. De hoogste risico's worden gevormd door leveranciers van cruciale IT- systemen en essentiële grondstoffen, zoals Managed Service Providers (MSP's), datacenters, hostingbedrijven, en leveranciers van kernbedrijfssoftware (bijvoorbeeld systemen voor boekhouding en klantbeheer). Een inbreuk bij deze leveranciers kan leiden tot ernstige verstoringen. Op een lager risiconiveau bevinden zich leveranciers van belangrijke technische installaties en infrastructuur, zoals installateurs van essentiële hardware en zonnepanelen, en transport- en distributiebedrijven. De impact van een incident bij deze groep hangt sterk af van de mate van afhankelijkheid van deze leveranciers. Het laagste risico wordt vertegenwoordigd door overige toeleveranciers. Echter, het belang van een gepersonaliseerde risicobeoordeling per organisatie blijft essentieel. Samen Digitaal Veilig biedt ondersteuning bij het beoordelen van deze risico's met onze risicoanalyse vragenlijst, waarmee leveranciers op basis van hun antwoorden in verschillende risicocategorieën worden ingedeeld."