NIS2 stap voorwaarts in Europese cyberbeveiliging

In het cyberbeveiligingslandschap komt de NIS2 richtlijn naar voren als een cruciale ontwikkeling, die het beschermingskader binnen de Europese Unie een nieuwe vorm geeft. Deze richtlijn gaat verder dan zijn voorganger en stelt verbeterde protocollen op om de steeds complexere aard van cyberdreigingen, waarmee entiteiten in verschillende sectoren worden geconfronteerd, aan te pakken en tegen te gaan.

Softwareontwikkelingsbedrijven opereren in de voorhoede van de technologische innovatie en ondervinden in het bijzonder de gevolgen van deze nieuwe regelgeving. Hun werk is inherent verweven met cyberbeveiliging en omvat veel processen die gevoelig zijn voor digitale bedreigingen. Deze bedrijven zijn verantwoordelijk voor het ontwikkelen van geavanceerde softwareoplossingen en het beschermen van de integriteit en privacy van de gegevens die deze oplossingen beheren.

Dit artikel ontleedt het proces van integratie van de nalevingseisen met betrekking tot de NIS2 richtlijn bij softwareontwikkelingsbedrijven.

Software-ontwikkelingsbedrijven onder de NIS2

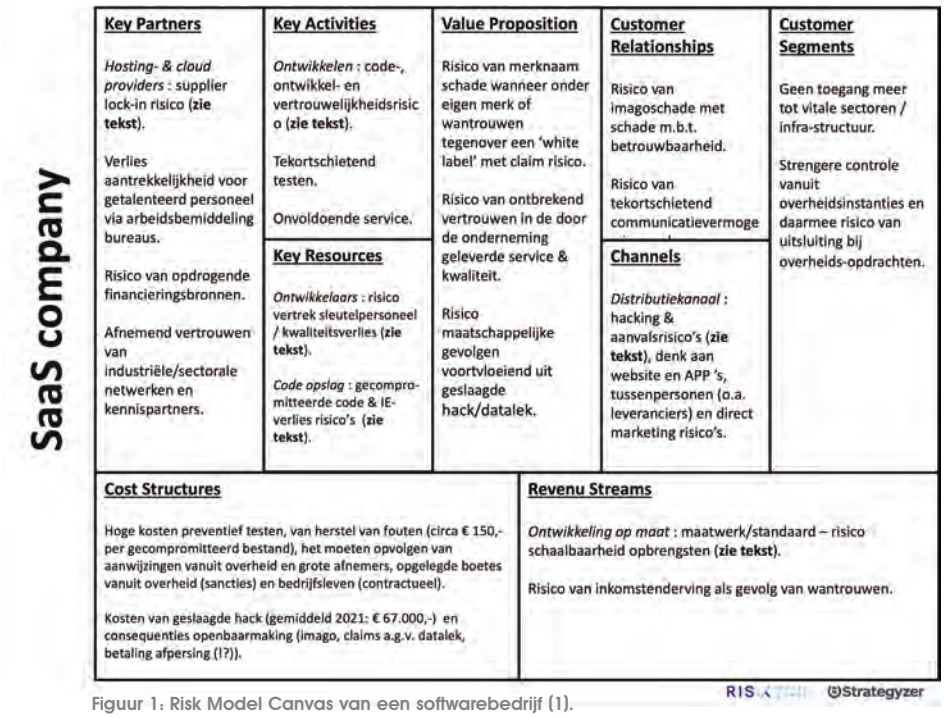
De NIS2 richtlijn werpt een breed net uit en richt zich op veel entiteiten die volgens de richtlijn 'essentieel' en 'belangrijk' zijn voor het maatschappelijk en economisch welzijn. Softwareontwikkelingsbedrijven vallen precies in deze categorie, als ze ook beheerde diensten leveren op de software die ze ontwikkelen (zoals SaaS-bedrijven). Als ruggengraat van de digitale infrastructuur zijn ze een integraal onderdeel wat het functioneren van verschillende sectoren betreft: van de gezondheidszorg tot de financiële sector. Hun platformen en applicaties verwerken vaak enorme hoeveelheden gevoelige gegevens, waardoor ze een spil vormen in het digitale ecosysteem en dus 'essentieel' zijn in de ogen van de richtlijn.

Risicogebaseerde benadering van cyberbeveiliging

NIS2 is een voorstander van een risicogebaseerde benadering van cyberbeveiliging. Dit betekent dat organisaties, in plaats van een pasklare oplossing voor te schrijven, hun specifieke kwetsbaarheden moeten evalueren en beveiligingsmaatregelen moeten bedenken, die in verhouding staan tot deze risico's. Deze benadering erkent de gevarieerde, dynamische aard van cyberbedreigingen en stelt softwareontwikkelingsbedrijven in staat om middelen plus verdedigingsmechanismen daar in te zetten waar ze het meest nodig zijn.

Belangrijkste vereisten voor naleving, gespecificeerd in artikel 21

Artikel 21 van NIS2 is de hoeksteen voor naleving; beschrijft de basismaatregelen die organisaties moeten nemen op het gebied van beveiliging en incidentrespons: van elementaire cyberbeveiligingspraktijken tot het opzetten van incidentresponsteams. Voor softwareontwikkelaars betekent dit dat ze ervoor moeten zorgen



Figuur 1: Risk Model Canvas van een softwarebedrijf (1).

dat hun ontwikkellevenscyclus, van ontwerp tot ingebruikname, is beveiligd tegen inbraak en gegevensschending.

Beveiliging toeleveringsketen en rapportage volgens NIS2

NIS2 gaat verder dan de direct betrokken organisatie, zij omvat de gehele toeleveringsketen. Softwareontwikkelaars moeten hun leveranciers en partners controleren op robuustheid van de cyberbeveiliging, waardoor een rimpeleffect van beveiligingsbewustzijn ontstaat. Bovendien is in het geval van een beveiligingsincident onmiddellijke rapportage verplicht - een vereiste die de nadruk van de richtlijn op transparantie en verantwoordingsplicht onderstreept.

Het bedrijfsmodel voor softwareontwikkeling

In het technologielandschap zijn softwareontwikkelingsbedrijven de architecten van digitale vooruitgang. Hun bedrijfsmodel is veelzijdig en gebouwd op een fundament van innovatie, technische bekwaamheid en strategische marktpositionering. Voor het ontleden van het businessmodel van een softwarebedrijf gebruiken we een Risk Model Canvas van de website riskmodelcanvas.net, zie figuur 1.

Kern bedrijfsstructuur softwareontwikkelingsbedrijf

Elk softwareontwikkelingsbedrijf moet beschikken over een goed geolied ontwikkelingsteam, verantwoordelijk voor de software-oplossingen; een operationeel team, dat zorgt voor soepele interne workflows en productlevering; en een marketingteam, die het bedrijf een stem geeft binnen een drukke markt. De combinatie van deze elementen bepaalt de huidige prestaties van het bedrijf en zet de koers uit voor de toekomstige groei.

Ontwikkeling is de drijvende kracht achter het aanbod van een softwarebedrijf en zet abstracte ideeën om in concrete producten. Operations ondersteunt de ontwikkelingscyclus, zorgt ervoor dat het eindproduct voldoet aan de kwaliteitsnormen en op tijd wordt geleverd. Aan de andere kant is marketing de stem van het bedrijf, belast met het positioneren van het product in de markt, het opbouwen van naamsbekendheid en het genereren van vraag. Samen ondersteunen deze drie pijlers de ambitie van het bedrijf om te innoveren en zijn bereik in het digitale domein uit te breiden.

Grote innovatie gaat echter ook gepaard met aanzienlijke risico's. Softwareontwikkelingsbedrijven bevinden zich in een

NIS2 erkent de complexiteit en het dynamische karakter van moderne cyberbedreigingen en biedt een flexibel, maar gestructureerd kader om deze aan te pakken

mijnenveld van potentiële bedreigingen, variërend van technische bedreigingen — zoals het handhaven van de kwaliteit van de code en bescherming tegen cyberbedreigingen – tot strategische dreigingen, zoals het voorblijven op snelle marktveranderingen en technologische vooruitgang. Diefstal van intellectueel eigendom, datalekken en verlies van menselijk kapitaal zijn ook belangrijke punten van zorg die het evenwicht van het bedrijfsecosysteem kunnen verstoren.

De risico's van het bedrijfsmodel

In het navolgend overzicht zijn de canvas thema's, gerelateerd aan risico's welke geclassificeerd zijn naar kans en impact. Dus van hoog (dagelijks tot maandelijks, regelmatig voorkomend) naar medium (enkele keren per jaar) naar laag (zelden). Daarbij de classificatie afgezet tegenover de impactklassen: financiële -, imago-, (wettelijke) regelgeving -, organisatorische - en veiligheidsrisico's. Ik ga hierbij niet in op de onderbouwing van het gehanteerde SaaS-classificatie voorbeeld.
Het Risk Model Canvas voor softwareontwikkeling beschrijft de bijbehorende bedrijfsrisico's (in het canvas indicatief voor de 9 thema's, hierna daarvan 5 thema's summier uitgewerkt):

Canvas thema: key partners

Canvas subthema: hosting- en cloud providers
Gerelateerd risico: supplier lock-in risico
Classificatie: medium
Beschrijving: bij de start vinden de kleinere SaaS-bedrijven en de providers elkaar, maar bij groei van het SaaS-bedrijf groeit niet altijd de provider mee. De provider moet aan nieuwe standaarden voldoen, maar dat lukt hen dan niet. De provider wordt dan de zwakste schakel. Een goed, volwassen leverancier selectie- en evaluatieproces is dan vereist.

Canvas thema: key activities

Canvas subthema: ontwikkelen
Gerelateerd risico: code- / ontwikkel- en vertrouwelijkheidsrisico
Classificatie: hoog
Beschrijving: problemen met de kwaliteit van de code leiden tot bugs, kwetsbaarheden en noodzaken tot patches en/of herstelwerkzaamheden. Niet daaraan verbonden problemen kunnen leiden tot cyberrisico's. Kwalitatief, goed codeerwerk leidt tot minder herwerking, meer innovatie en hogere bedrijfsinkomsten. Dat laatste verschil kan meer dan 10% uitmaken en dus behoort codering van goede kwaliteit tot de kern van de dagelijkse activiteiten van een SaaS-bedrijf. Denk echter ook aan vitale sectoren (hoog strategische/fatale incidenten impacts), waar overheid regulerend optreden zal.

Canvas thema: key resources

Canvas subthema: ontwikkelaars
Gerelateerd risico: risico vertrek sleutelpersoneel/kwaliteitsverlies
Classificatie: medium
Beschrijving: een bureaucratische benadering van de schaarse ontwikkelaars, waaronder de hooggekwalificeerde en -getalenteerde Neuro Diverse Persoonlijkheden, zullen deze verjagen. Vaak zijn deze conceptueel gerichte denkers wars van (werk)procedures en documentalisering, terwijl ze tegelijkertijd als geen ander de noodzaak van informatiebeveiliging begrijpen en als persoonlijke noodzaak ervaren. Een pragmatische benadering van deze tegenstrijdigheid bij implementatie van informatiebeveiliging en de eis van compliance moet worden gevonden.

Canvas subthema: code opslag
Gerelateerd risico: gecompromitteerde code en IE-verlies risico's
Classificatie: medium
Beschrijving: kleinere SaaS-bedrijven (MKB) concentreren hun aandacht te veel op de operatierisico's (productieomgeving/werkterrein) in plaats aandacht te behouden voor de code repository, waarvan compromittering kan leiden tot Intellectueel Eigendom (IE-)verlies. Ontwikkelaars en hun laptops zijn een belangrijke risico-aspect. Een concreet voorbeeld: de consequenties van de Russisch-Oekraïense oorlog voor bedrijven met zowel Russische als Oekraïense ontwikkelaars. Een ander essentieel risico: bedrijfsdiscontinuïteit bij verlies van toegang tot de code repository! De beschikbare oplossingen zijn er, maar zeker niet eenvoudig te implementeren.

Canvas thema: channels

Canvas subthema: distributiekanaal
Gerelateerd risico: hacking- & aanvalrisico's
Classificatie: hoog
Beschrijving: een geslaagde hack of aanval schaadt de beschikbaarheid, vertrouwelijkheid en/of integriteit van de informatie. Afhankelijk van de aard van de op het SaaS-platform opgeslagen informatie kan gerichte aanvallen plaatsvinden. Herstel daarvan is vaak kostbaar, gezien de gemiddelde herstelkosten - per gecompromitteerd bestand circa 150 euro - en dat los van de imagoschade. Hackers mogen niet eenvoudig toegang kunnen verkrijgen. Kosten en imagoschade leiden tot inkomstenderving, het risico is dus hoog.

Canvas thema: revenu streams

Canvas subthema: ontwikkeling op maat/standaard
Gerelateerd risico: maatwerk/standaard – risico schaalbaarheid opbrengsten
Classificatie: hoog
Beschrijving: op korte termijn levert software-aanpassing snel inkomsten, op lange termijn kan het lastiger uitvallen en inkomsten doen verminderen. Denk aan de verder ontwikkeling van het kernproduct, leidende tot noodzakelijk onderhoud van de al gerealiseerde aanpassingen, dat voor rekening van het bedrijf komt tenzij er een onderhoudscontract is overeengekomen. In geval van maatwerkoplossingen zal onderhoud aandacht en tijd claimen, waardoor innovatie van het kernproduct kan stagneren. Maatwerk kan vanuit beveiligingsoogpunt riskant blijken te zijn, doordat risico's op bugs en operationele problemen toenemen.

Minimale vereisten NIS2 richtlijn en risico's

NIS2 gaat over risicobeheer. Dus om de minimale maatregelen van NIS2 correct te implementeren, moeten we risico's afstemmen op de minimale vereisten van de NIS2 richtlijn. Laten we de typische risico's analyseren waarmee dergelijke bedrijven te maken hebben en hoe ze zich verhouden tot de richtlijnen, gevolgd door suggesties voor het implementeren van deze vereisten. Let op: dit is een voorbeeld; risico's zijn voor elk bedrijf anders.

Risicothema: kwaliteit van code(-ontwikkeling)

Minimum eis NIS2 - e: veiligheid systemen
Classificatie: hoog
Analyse en implementatie: coderingsstandaarden en regelmatige codebeoordelingen toepassen om kwaliteit te waarborgen. Beleidsintegratie voor het omgaan met en het openbaar maken van kwetsbaarheden, dat aansluit bij de focus van NIS2 op beveiliging bij het verkrijgen, ontwikkelen en onderhouden van systemen.

Risicothema: hacking en aanval

Minimum eis NIS2 - b: incidentafhandeling
Classificatie: hoog
Analyse en implementatie: ontwikkel een incidentbestrijdingsplan met directe beheersings- en uitroeiingsstappen. Train het incidentresponsteam regelmatig, volgens de protocollen voor incidentafhandeling van NIS2, om aanvallen effectief af te handelen.

Risicothema: aanpassing versus standaardisatie

Minimum eis NIS2 - f: effectiviteit cyberbeveiligingsmaatregelen
Classificatie: hoog
Analyse en implementatie: stel een raamwerk op om de beveiliging van aangepaste ontwikkelingen continu te evalueren. Voer effectbeoordelingen uit voor elke aanpassing, rekening houdend met onderhoud op lange termijn en de extra risico's die ze kunnen introduceren.

Risicothema: behoud van gekwalificeerd personeel

Minimum eis NIS2 - g: basis cyberhygiëne en -training
Classificatie: medium
Analyse en implementatie: bevorder een beveiligingscultuur, die de inbreng van ontwikkelaars waardeert. Bied cyberbeveiligingstrainingen aan op maat voor ontwikkelaars om ervoor te zorgen dat beveiligingspraktijken hun tevredenheid niet in de weg staan, zodat talent behouden blijft.

Risicothema: code repository en IE

Minimum eis NIS2 - a: risicoanalyse en beveiliging informatiesysteem
Classificatie: medium
Analyse en implementatie: beveilig code-opslagplaatsen met toegangscontroles. Maak regelmatig back-ups van de repositories en controleer ze om IE-verlies te voorkomen, dit in overeenstemming met de risicoanalyse en het systeembeveiligingsbeleid van NIS2.

Risicothema: hosting- en cloudproviders

Minimum eis NIS2 - d: veiligheid van de toeleveringsketen
Classificatie: medium
Analyse en implementatie: grondige beveiligingsbeoordelingen van hosting- en cloud providers uitvoeren. Ervoor zorgen dat ze voldoen aan de NIS2-nalevingsnormen of deze overtreffen en continue bewaking voor compliance-afwijkingen inbouwen.

Suggesties voor implementatie op basis van risico

Besluit op basis van de in kaart gebrachte risico's de volgende maatregelen voor elk risico op hoog niveau:

1. **supplier lock-in risico:**
   - o Neem clausules op in contracten met hosting- en cloudproviders die naleving van specifieke beveiligingsstandaarden en regelmatige rapportage verplichten.
   - o Plan regelmatige bijeenkomsten met providers om de beveiligingsmaatregelen en naleving van de nieuwste standaarden te bespreken.
2. **code- / ontwikkel- en vertrouwelijkheidsrisico:**
   - o Stel strikte coderingsrichtlijnen op en voer regelmatig controles uit om naleving te garanderen.
   - o Continue integratie en implementatie (CI/CD) pipelines borgen, die geautomatiseerde beveiligingsscans bevatten.
3. **risico vertrek sleutelpersoneel/kwaliteitsverlies:**
   - o Ontwikkel een aantrekkelijk trainingsprogramma voor cyberbeveiliging met gamification en beloningen om naleving van de beveiliging te stimuleren.
   - o Flexibele beveiligingstools en -praktijken implementeren die integreren met de workflows van ontwikkelaars, waardoor wrijving en weerstand worden verminderd.
4. **gecompromitteerde code en IE-verlies risico's:**
   - o Gebruik veilige, gerenommeerde platforms voor codeopslagplaatsen met multi-factor authenticatie en regelmatige toegangscontroles.
   - o Stel als beleid vast, dat alle code wordt beoordeeld en getest voordat het wordt samengevoegd in het kernproduct.
5. **hacking- & aanvalrisico's:**
   - o Ontwikkel een robuust kader voor incidentafhandeling met detectie-, rapportage- en herstelprocessen ten aanzien van mogelijke inbreuken.
   - o Voer regelmatig penetratietests en red team-oefeningen uit om aanvallen te simuleren en responsstrategieën te verfijnen.
6. **maatwerk/standaard – risico schaalbaarheid opbrengsten:**
   - o Voordat een project start is het te adviseren een protocol voor aangepaste ontwikkeling te introduceren, dat ook een risicobeoordelingsfase omvat.
   - o Realiseer een versiecontrolesysteem dat alle wijzigingen logt en in geval van problemen het systeem terug kan zetten naar een stabiele staat.

Taken voor reactie op incidenten en rapportage

Artikel 23 van de NIS2 richtlijnen geeft duidelijk aan hoe en hoe snel organisaties incidenten moeten melden. Deze vereisten zijn geweldig om op te nemen en te bekijken in jouw incident response plan.

Hieronder volgt een samenvatting:

- **Melding van incidenten:** instanties moeten elk belangrijk incident, dat een impact heeft op hun diensten onmiddellijk melden. Dit omvat een vroegtijdige waarschuwing binnen 24 uur en een gedetailleerde melding van het incident binnen 72 uur.
- **Communicatie:** als er een significante cyberdreiging is, moeten entiteiten de beschikbare tegenmaatregelen communiceren naar de getroffen ontvangers van services.
- **Criteria voor een belangrijk incident:** een incident wordt als significant beschouwd als het resulteert in ernstige operationele verstoring of financieel verlies of als het andere partijen kan treffen door aanzienlijke schade te veroorzaken.
- **Terugkoppeling:** het CSIRT of de bevoegde autoriteit moet binnen 24 uur na een vroegtijdige waarschuwing reageren naar de aanmeldende entiteit.
- **Bewustmaking van het publiek:** als bewustmaking van het publiek nodig is, kan het CSIRT of de bevoegde autoriteit van een lidstaat het publiek informeren of de entiteit vragen dit te doen.
- **Samenvattende verslagen:** elke drie maanden moet het centrale contactpunt een samenvattend verslag indienen bij ENISA.
- **Uitvoeringshandelingen:** tegen 17 oktober 2024 zal de Commissie specificeren in welke gevallen een incident als significant wordt beschouwd.
- **Begeleiding:** het CSIRT of de bevoegde autoriteit zal begeleiding of operationeel advies geven over de implementatie van mogelijke risicobeperkende maatregelen.

Conclusie

Na een grondige verkenning van de NIS2 richtlijn en de implicaties ervan op software-ontwikkelingsbedrijven, is het duidelijk dat deze richtlijn een aanzienlijke stap voorwaarts betekent in de evolutie van cyberbeveiliging binnen de Europese Unie. De risicogebaseerde benadering, die centraal staat in NIS2, is een krachtige strategie die bedrijven stimuleert om een meer op maat gemaakte, dynamische benadering van cyberbeveiliging te hanteren. Dit is niet alleen effectiever in een steeds veranderend dreigingslandschap, maar het moedigt ook innovatie en proactieve beveiligingspraktijken aan.

Een ander sterk punt van NIS2 is de nadruk op de beveiliging van de toeleveringsketen. Door de focus te verbreden van individuele organisaties naar hun netwerk van leveranciers en partners, versterkt NIS2 de algehele veerkracht van de digitale infrastructuur tegen cyberbedreigingen.

Hoewel de richtlijn een kader biedt, blijft de specifieke uitvoering ervan in veel gevallen open voor interpretatie. Dit kan leiden tot inconsistenties in hoe bedrijven de richtlijn naleven en hoe toezichthouders deze handhaven. Persoonlijk vind ik een groot gedeelte van de richtlijn maar vaag en de minimale eisen lijken niet sterk te zijn opgezet: elke eis bestaat eigenlijk uit meerdere eisen en het is maar vreemd in elkaar verweven.

Toch ben ik van mening dat NIS2 een positieve stap voorwaarts is in het versterken van de cyberbeveiligingsinfrastructuur binnen de EU. De richtlijn erkent de complexiteit en het dynamische karakter van moderne cyberbedreigingen en biedt een flexibel, maar gestructureerd kader om deze aan te pakken. De uitdagingen in de implementatie zijn echter niet te negeren en vereisen voortdurende aandacht en mogelijk aanpassingen om te zorgen voor effectieve en haalbare naleving, vooral voor kleinere organisaties. Zoals met elke grootschalige regelgevende inspanning, zal het succes van NIS2 afhangen van de samenwerking tussen alle belanghebbenden, de duidelijkheid van richtlijnen en de bereidheid om te leren en aan te passen naarmate de tijd vordert.

Referentie

(1) https://riskmodelcanvas.net/saas-company