Dit bericht is anoniem, want hierin worden een aantal pijnpunten opgenoemd waarin overheid en het bedrijfsleven ernstig tekortschieten.

Ik zelf ben software ontwikkelaar en verantwoordelijk voor systemen waar bijzondere persoonsgegevens op staan.

De NIS2 is prima, doch irrelevant

De NIS2, hoewel goed bedoelt en zeker inhoudelijk aantrekkelijk, is irrelevant. Net als de AVG en andere wetgeving. Kritiekpunten die ik heb over de NIS2 sluiten aan met die van het bericht van de anonieme gebruiker uit Arnhem op 29 mei 2024, dus ik sluit mij daar bij aan.

Waarom de NIS2 irrelevant is, is als volgt:

Nederlandse ICT veiligheid is extreem ondermaats, en er is amper toezicht.

De overheid, en de Europese Unie, hebben in het verleden meerdere wetten en regelementen aangenomen waarin overheidsinstanties en bedrijven worden geboden het beheer van persoonlijke gegevens en kritische systemen veilig te beheren, denk aan bijvoorbeeld de AVG.

Cyberbeveiliging en het verzekeren dat systemen operationeel zijn, zijn hier ook onderdeel van. Het probleem is echter; als niemand de wet volgt, is het geen oplossing om meer wetten aan te leggen. Er is zeer gebrekkig overzicht of bedrijven wel de wet volgen, en de Autoriteit Persoonsgegevens en andere instanties komen pas in actie als het kwaad al geschied is. Er word dan een boete uitgedeeld, maar het kernprobleem word niet opgelost. En als de boetes minder ernstig zijn dan de kosten voor implementaties van veiligheid, dan voldoet de wet niet.

Laten we een analogie maken: in de wet staat dat iedereen een autogordel moet dragen. Draagt iemand die niet en komt terecht in een auto-ongeluk, dan heeft dat als consequentie dat diegene schade (gedeeltelijk) voor eigen rekening moet nemen. Maar dat neemt niet weg dat het doden tot gevolge heeft en men de sloot dempt als het schaap verdronken is. “Ik draag geen autogordel, ik heb nooit een ongeluk gehad!” is dan excuus die genoemd word. Daarom surveilleert de politie en deelt boetes uit aan degenen die de autogordel niet dragen.

Voor cyberbeveiliging, echter, is er geen surveillance. Er zijn veel aanbieders in Nederland die computerprogramma’s aanleggen, onderhouden en aanbieden waarvan de veiligheid niet word gecontroleerd. Niemand weet wat er achter de schermen plaatsvind. De overheid en grote bedrijven kopen vervolgens deze diensten in voor beheer en verwerking van persoonsgegevens – vaak ook bijzondere persoonsgegevens (volgens AVG wetgeving). Gegevens waarvan soms kwaadaardige partijen de inhoud willen weten. Denk bijvoorbeeld aan criminelen of buitenlandse mogendheden. Dit houd dus in dat niet alleen de privacy van mensen makkelijk op straat ligt, maar in sommige gevallen dus ook hun veiligheid.

Als ontwikkelaar heb ik dit bij voormalige werkgevers zien gebeuren: onze klanten waren o.a. overheidsinstanties, inclusief defensie, de politie en rechtbanken. Ook grote bedrijven – waaronder veiligheidsbedrijven - waren vaak klant en gebruikten het product voor de verwerking/opslag van belangrijke data, ook via de servers gedraaid en onderhouden door de werkgever. Er was echter sprake van slecht wachtwoordbeheer, slechte beveiliging op de servers, slechte beveiliging in de code, gebrek aan onderhoud van beveiligingsupdates en ga

maar verder. En niemand die vragen stelde. (Denk aan code gevoelig voor SQL injecties, .NET versies waar Microsoft geen veiligheidsupdates voor uitbrengt, misbruik vanuit de browser, geen server controle voor input van een client applicatie, enz.). Ook waren de systemen slecht onderhouden en soms vlogen componenten er uit door slecht programmeerwerk (memory leaks bijvoorbeeld).

Dit zijn geen geïsoleerde incidenten, maar een fenomeen dat zich overal afspeelt. Buitenlandse mogendheden waarmee Nederland slechte diplomatieke betrekkingen heeft kunnen gewoonweg op allerlei servers rondwandelen en data stelen, en niemand die wijzer word. Hetzelfde geld voor criminelen. Ransomware hackers kunnen overal binnenlopen en systemen omver halen. Iedere dag is er wel weer ergens een nieuw incident; trek maar een krant open. En aangezien veiligheidsmaatregelen veel geld kosten en bijna niemand het doet, en de boetes relatief laag zijn mocht het fout gaan, zien bedrijven geen noodzaak hun veiligheid op orde te hebben.

Pak voor de broek voor de AIVD:

Ik vind het ronduit stuitend dat de AIVD zich niet richt op het feit dat al deze bedrijven en instanties niet de veiligheid van persoonsgegevens en kritische systemen op orde hebben zoals aangegeven in de AVG en andere wetgeving. Ik vind het twijfelachtig dat ze dat niet doorhebben, en als ze dat echt niet doorhebben, vraag ik me af hoe competent ze eigenlijk zijn in Zoetermeer. Het zou hun prioriteit moeten wezen dat de bedrijven en instanties alles op orde moeten hebben voor de bescherming en beschikbaarheid van data van Nederlandse burgers, en hier toezicht op houden. Zeker als de Kamer wil dat zij bedrijven inlichten over potentiële hackpogingen. (En zelfs al zou dit niet in hun takenpakket liggen, dan zouden ze sowieso hierover moeten blijven hameren bij de politiek dat iemand het op zich moet nemen)

Het feit dat het uitgerekend Nederlandse gebruikers van 4Chan zijn – de ‘extreemrechtse plek’ waar de AIVD ieder jaar over rapporteert – die regelmatig aanhalen dat de beveiliging van bedrijven/instanties niet op orde zijn en zorgen uiten dat deze buitenlandse mogendheden hier misbruik van (kunnen) maken, zou zeer hilarisch zijn als het niet zo triest was. Misschien moeten ze hen maar de leiding laten geven over de ICT afdeling van de AIVD, want die gebruikers lijken meer bezorgd over de veiligheid van ICT systemen in Nederland dan de AIVD zelf.

Pak voor de broek voor alle overheidsinstanties, voornamelijk de politie, marechaussee, defensie en rechtbanken:

Jullie kopen regelmatig software in van derde partijen zonder vragen te stellen. Geen audits, geen certificatie, geen niks. Ik heb dit met mijn eigen 2 ogen zien gebeuren. We weten allemaal van de euvels rondom de communicatiesystemen bij de politie, maar dit is slechts het topje van de ijsberg.

De oplossing; een nieuwe toezichthouder.

Net als de NVWA, de Agentschap Telecom, de Inspecties en Staatstoezicht op de Mijnen moet er ook een toezichthouder zijn voor ICT beveiliging. Noem het ‘Inspectie ICT Beveiliging’ o.i.d. Deze zou van toepassing moeten zijn voor alle bedrijven/overheidsinstanties die:

- Persoonsgegevens op grote schaal verwerken.
- Bijzondere persoonsgegevens verwerken, ongeacht de schaal.
- Persoonsgegevens verwerken voor kwetsbare personen.
- Kritische systemen draaien waarvan de samenleving afhankelijk is.

Hiervan moet geëist worden dat:

- Ze gecertifieerd zijn door erkende auditors voor het werk dat ze doen, denk aan bijvoorbeeld ISO 27001 of IASME.
- Ze regelmatig gecontroleerd worden voor audits door 3e partijen die de overheid erkent als geschikte auditor. De regelmaat is afhankelijk van de hoeveelheid en de ernst van de persoonsgegevens die verwerkt word door het bedrijf, of hoe ontwrichtend het is als hun systemen uitvallen.
- Bij grootbedrijven (dus niet MKB's) een gecertificeerde interne auditor die werkt als de Data Security Officer.
- Het bedrijf moet incidenten goed documenteren voor inzage. Het niet documenteren van incidenten of valsheid in geschrifte moet hard aangepakt worden.

Deze richtlijnen zouden dan voor alle bedrijven moeten gelden die software ontwikkelen en/of systemen beheren en aan de voorwaarden voldoen. Dit geld dus ook voor bedrijven die code ontwikkelen voor eigen gebruik waarbij persoonsgegevens/kritische systemen verwerkt worden.

Uiteraard kan dit allemaal niet 1-2-3 geregeld worden, en er zijn zo weinig bedrijven die op dit moment aan de voorwaarden voldoen dat het gewoon triest is. Daarom zou er moeten worden ingesteld dat alle bedrijven een paar jaar de tijd krijgen aan de voorwaarden te voldoen, en pas daarna in te haken. Als het nodig is zou er kunnen worden overwogen dat bedrijven subsidies/belastingaftrek kunnen aanvragen voor de onkosten van certificering.

Als een bedrijf niet aan de voorwaarden voldoet, kan er een waarschuwing gegeven worden dat het bedrijf binnen een periode de problemen moet hebben opgelost. Als de veiligheid ondermaats blijft, dan mogen de producten/diensten van het bedrijf niet meer benut worden door zowel overheidsinstanties als het bedrijfsleven totdat het bedrijf alles weer op orde heeft.

Dit is zeer streng, maar noodzakelijk: kijk en huiver: https://www.datalekt.nl/home/overzicht-alle-cyber-incidenten/ (en dit zijn slechts incidenten die we kennen en niet onder de mat zijn geschoven door het bedrijf!).

We kunnen de put niet blijven dempen voor ieder dood schaap! Misschien is het maar eens tijd een hek aan te leggen.