Overzicht meldplichten bij ransomware

AVG
In Nederland geldt sinds 2016 een meldplicht voor datalekken voortkomend uit de Europese Algemene Verordening Gegevensbescherming (AVG). Dit houdt in dat organisaties (zowel bedrijven als overheden) direct een melding moeten doen bij de Autoriteit Persoonsgegevens (AP) zodra zij een ernstig datalek hebben. Van een datalek is sprake wanneer een inbreuk op de beveiliging leidt tot ongeoorloofde of onbedoelde verstrekking van of toegang tot persoonsgegevens. Maar ook als de inbreuk ertoe leidt dat deze gegevens ongewenst of onrechtmatig zijn vernietigd, verloren, of gewijzigd. Organisaties die getroffen zijn door een datalek kunnen dit melden via het meldformulier datalekken op de website van de AP. Wanneer het datalek een hoog risico vormt voor de personen wiens data is getroffen dient de organisatie daarnaast ook die personen te informeren zodat zij zich kunnen wapenen tegen de gevolgen. Data die bij een ransomware aanval wordt ontvreemd, kan bijvoorbeeld misbruikt worden voor het versturen van spam- en (spear)phishing berichten en het plegen van identiteitsfraude en oplichting. De AP kan handhavend optreden als organisaties personen wiens data is getroffen niet informeren.

Wbni
De Wet beveiliging netwerk- en informatiesystemen (Wbni) is in 2018 in werking getreden en betreft in hoofdzaak de implementatie van de Europese Netwerk- en informatiebeveiligingsrichtlijn (NIB-richtlijn). De Wbni bevat een zorgplicht en een meldplicht voor aanbieders van essentiële diensten (AED's) en digitale dienstverleners (digital service provider, DSP's). Deze dienstverleners moeten ernstige ICT-incidenten melden aan het Nationaal Cybersecurity Centrum (NCSC) of het CSIRT voor digitale dienstverleners voor eventuele incident ondersteuning en bij de sectorale autoriteit die belast is met toezicht en handhaving. Het doel van deze meldplicht is om autoriteiten op de hoogte te stellen van incidenten met (mogelijke) ernstige maatschappelijke en economische gevolgen, zodat zij daar op kunnen reageren.

In de Wbni wordt een meldplichtig incident gedefinieerd als een incident dat aanzienlijke gevolgen heeft voor de continuïteit van zijn essentiële dienst. Hierbij wordt rekening gehouden met verschillende factoren, zoals het aantal gebruikers dat door de verstoring van de dienst wordt getroffen, de duur van het incident en de omvang van het geografische gebied dat door het incident wordt getroffen. Deze factoren kunnen op sectoraal niveau verder uitgewerkt zijn door de beleidsverantwoordelijke minister. Een aanval met ransomware kan daarmee leiden tot een meldplichtig incident in de zin van de Wbni. Organisaties kunnen daarnaast ook een vrijwillige melding doen bij het NCSC.

In december 2022 is de NIS2-richtlijn vastgesteld, de opvolger van de huidige NIB-richtlijn. Het kabinet werkt onder mijn coördinatie momenteel aan een wetsvoorstel ter implementatie van de NIS2-richtlijn. Als gevolg van deze richtlijn zullen in Nederland veel meer organisaties te maken krijgen met verplichtingen voor hun cybersecurity, waaronder een meldplicht voor significante incidenten. Onderdeel van deze meldplicht is de verplichting voor organisaties die onder deze richtlijn vallen om afnemers van hun diensten te informeren over incidenten die een nadelige invloed kunnen hebben op de verlening van hun diensten.