Toezichthouder AP ziet vaak ‘dubbele afpersing’ bij ransomware.

Bij de Autoriteit Persoonsgegevens zijn vorig jaar 178 aanvallen met ransomware gemeld, de gijzelsoftware waarmee cybercriminelen netwerken platleggen om losgeld te eisen. ‘Dubbele afpersing’, waarbij sprake is van een vergrendeling van de systemen en datadiefstal, is in opkomst.

Het daadwerkelijke aantal slachtoffers ligt waarschijnlijk op ‘vele honderden’, omdat een enkel getroffen bedrijf vele klanten kan hebben die ook geraakt worden, stelt de toezichthouder in zijn eerste onderzoek naar deze gijzelsoftware.

De aanvallen met ransomware zijn uiterst schadelijk voor bedrijven. Het kost veel tijd en geld om de indringers uit de systemen te werken en er zijn mogelijk ook persoonsgegevens bij betrokken. Aanvallen met ransomware troffen op die manier vorig jaar de gegevens van ‘miljoenen Nederlanders’, volgens de AP.

Online verspreiden.

De toezichthouder zag vorig jaar ‘een trend van dubbele afpersing’ in Nederland. Bij ongeveer de helft van negentig onderzochte bedrijven gingen de systemen op slot, maar werden ook data zoals persoonsgegevens ontvreemd. Bedrijven moesten vervolgens dubbel betalen, om systemen te ontgrendelen en te voorkomen dat gegevens online verspreid zouden worden.

Bij twee derde van de slachtoffers kwamen de indringers binnen doordat bedrijven het basisniveau van beveiliging niet volgden, aldus de toezichthouder. Ze verzuimden software tijdig te updaten, voerden een slecht wachtwoordbeleid of het ontbrak aan meerfactorauthenticatie.

Van de groep onderzochte bedrijven betaalde 9% losgeld. Dat zo weinig bedrijven betalen is een positief signaal, vindt de toezichthouder, omdat betaling ‘een illegaal systeem in stand houdt’. Bovendien betekent betaling geen garantie dat systemen weer vrij komen, zoals ten minste één Nederlands bedrijf vorig jaar merkte. Een grotere groep van 62% zegt wel onderhandeld te hebben over het betalen van losgeld.

In ongeveer de helft van de onderzochte gevallen was de indringer maximaal zes dagen binnen in de systemen van een bedrijf. Bij vijf gevallen ging het om meer dan 120 dagen.

Project Melissa.

Het aantal meldingen van de AP is hoger dan de schatting van project Melissa, een samenwerkingsverband van cyberbeveiligingsbedrijven en de overheid om bedrijven te helpen met het bestrijden van ransomware. Zij spraken eerder dit jaar over 147 aanvallen in 2023.

Het ging daarbij echter om aanvallen op bedrijven met meer dan honderd medewerkers. Een ander verschil is dat project Melissa kijkt naar meldingen bij aangesloten bedrijven en opsporingsinstanties. Bedrijven die een datalek hebben door ransomware hoeven zich daar niet te melden, maar zijn wettelijk wel verplicht een melding te doen bij de AP.

'Het aantal hele grote aanvallen bij grote bedrijven neemt af, vooral mkb'ers worden vaker getroffen', signaleert Arwi van der Sluijs, directeur van cyberbeveiliger Nfir en een van de initiatiefnemers van Melissa. 'Veel aanvallen met ransomware kwamen uit Oekraïne en Rusland. Sinds de oorlog zien cyberbeveiligers een decimering van het aantal grote aanvallen vanuit die landen.'

Oekraïne werkt de laatste jaren meer samen met Europese opsporingsinstanties om cybercriminaliteit tegen te gaan. Dat was in mei ook te zien bij het oprollen van een ransomwarenetwerk, dat voornamelijk vanuit dat land actief was. Bij deze 'grootste operatie tegen ransomware ooit', volgens opsporingsinstanties Eurojust en Europol, was project Melissa ook betrokken. Vorig jaar was het Nederlandse samenwerkingsverband betrokken bij het oprollen van vier dergelijke ransomwarenetwerken, stelt Van der Sluijs.