COLUMN | JASPER HULSEBOSCH

Jasper Hulsebosch is een ervaren advocaat met een internationale praktijk op het gebied van IE/IT en met een focus op het gebied van privacy, cybersecurity, anti-piracy en brand protection. Hij is partner bij De Vos & Partners Advocaten.

Reageren op een cyberaanval

IT-incidenten kunnen de samenleving ontwrichten. Zo was de website van de Rechtspraak eerder dit jaar onbereikbaar vanwege een DDoS-aanval en werd MediaMarkt slachtoffer van ransomware waarbij $ 50 miljoen losgeld zou zijn geëist. De toename van het aantal thuiswerkers vanwege de COVID19-pandemie en de opkomst van IoT en cloud computing hebben geleid tot een toename van (geslaagde) digitale aanvallen.

Er komt dan ook steeds meer (en strengere) cybersecuritywetgeving met vergelijkbare beveiligingseisen en meldplichten zoals we die al kennen uit de privacywet AVG. Vitale aanbieders en 'Digital Service Providers' moeten al sinds 2018 passende technische en organisatorische maatregelen treffen om hun IT te beveiligen en ernstige IT-incidenten melden bij de toezichthouders. In de toekomst zullen dit soort verplichtingen voor meer bedrijven gaan gelden. De toename van cyberaanvallen en cybersecuritywetgeving noopt niet alleen tot passende beveiligingsmaatregelen. Het is ook van belang (intern) beleid op te stellen dat helpt adequaat te reageren op incidenten, ook wel genoemd: een 'Incident Response Plan' (IRP). Een IRP is onmisbaar omdat bij een IT-incident vele zaken tegelijkertijd spelen en op bepaalde punten snelle beslissingen vereist zijn. Moeten bijvoorbeeld IT-systemen worden ontkoppeld, aangifte worden gedaan en melding worden gedaan bij toezichthouder(s) en betrokkenen?

Bij een IRP worden – kort samengevat – onder meer de volgende stappen gezet:

- de CISO of een externe cybersecurity deskundige stelt eerst vast of daadwerkelijk sprake is van een IT-incident ('Indicators of Compromise');
- er wordt een speciaal IRP-team samengesteld dat tijd en budget heeft om het IT-incident verder te onderzoeken en af te handelen, veelal bestaande uit de CISO, de FG, iemand van de afdeling PR/Communicatie en Legal en, indien nodig, aangevuld met een externe cybersecuritydeskundige of advocaat;
- dagelijks overleg door het IRP-team over diverse onderwerpen waarbij wordt gerapporteerd aan de directie, zoals de wijze van communicatie over het IT-incident, digitaal forensisch onderzoek (veilig stellen bewijsmateriaal), het nemen van mitigerende maatregelen, of er wettelijke verplichtingen zijn het IT-incident te melden aan de AP, betrokkenen (consumenten) en/of andere toezichthouders (zoals NCSC/CSIRT), het informeren van verzekeraars en het doen van aangifte.

Adequate reactie

Anno 2021, waar cyberaanvallen aan de orde van de dag zijn, is een IRP inmiddels noodzaak. De vraag is immers niet of een bedrijf slachtoffer wordt van een cyberaanval, maar wanneer. Een IRP zorgt voor een adequate reactie op een IT-incident en kan schade beperken (ook vanuit PR-oogpunt!), helpen bij het voldoen aan (wettelijke) meldplichten en bedrijven indirect dwingen passende beveiligingsmaatregelen te treffen voor de toekomst.