Beter anoniem melden

Advocaat Aldo Verbruggen stipt in het FD van 24 oktober aan dat de meldplicht datalekken in de huidige vorm van de baan moet. Het loont niet om een datalek te melden door het risico op grote reputatieschade en een hoge boete. Een ander belangrijk argument blijft nog onbelicht. Vooralsnog zijn er zeer weinig meldingen bij het meldloket datalekken binnengekomen. De overheid creëert hiermee vooral een gevoel van schijnveiligheid. Bedrijven krijgen door het lage aantal meldingen onterecht het idee dat cybercrime geen ernstige zaak is. Ze horen de waarschuwingen van securityleveranciers, de AIVD en een handjevol politici dan ook gelaten aan. Dikwijls ervaren ze zelf ook nog geen problemen. Bedrijven beseffen echter niet dat cybercriminelen vaak al in hun netwerken geïnfiltreerd zijn. Zeker in het geval van bedrijfsspionage doen indringers er alles aan om onopgemerkt te blijven. Daarnaast hebben online criminelen vaak data in handen waarvan de toekomstige waarde nog onbekend is. Als het huidige systeem ons iets heeft geleerd, is het dat bedrijven bij het melden van incidenten het risico op reputatieschade groot achten. Een systeem dat (anoniem) melden faciliteert, geen extra risico oplevert, en bij voorkeur zelfs beloont, brengt ons dichter bij het uiteindelijke doel: een actueel beeld van cybercriminaliteit, zodat we ons hiertegen kunnen wapenen.

Erik Ploegmakers, managing director KPN Security Services

Bescherming privacy

Verbruggen zegt regelmatig te adviseren om geen melding te maken van datalekken bij de Autoriteit Persoonsgegevens, onder andere omdat dit niet bijdraagt aan opsporing van cybercrime. Opsporing is echter niet het primaire ontstaansrecht van de meldplicht datalekken, de bescherming van het fundamentele recht op privacy is dat wel. Hiertoe is de meldplicht in tweeën gesplitst. Het eerste doel is preventie – de afschrikwekkende werking dient ertoe te leiden dat bedrijven en overheden hun beveiliging verbeteren. En dat helpt: een datalek van persoonsgegevens die met encryptie beveiligd zijn moet enkel aan de Autoriteit worden gemeld en komt daarmee niet in de openbaarheid. Dat laten de 4000 meldingen al zien, weinig daarvan zijn bekend.

Pas als een datalek ook gevolgen heeft voor de privacy van betrokken personen dient dit openbaar gemaakt te worden. Zijn hun accountgegevens gehackt? Of persoonsgegevens vernietigd zonder dat daarvan een kopie is gemaakt? Het fundamentele recht op privacy betekent dat personen dit moeten weten om zelf maatregelen te kunnen nemen. Dit is het tweede doel van de Meldplicht. Al met al genoeg reden om deze in acht te nemen.

Annemarie Bloemen, partner bij Grasp

Zorgplicht serieus nemen

Bedrijven die gevoelige informatie hebben van hun klanten moeten daar goed voor zorgen. Als er een datalek is geconstateerd, dan is het melden daarvan aan je klanten ‘the right thing to do’. Klanten moeten jou als organisatie kunnen vertrouwen. En ook al leidt dat niet tot vervolging en veroordeling van de dader, als bedrijf/organisatie moet je je zorgplicht serieus nemen en niet alleen communiceren in goede tijden maar ook in slechte tijden. Misschien zal op korte termijn de openheid over een datalek leiden tot het afnemen van het vertrouwen, maar op lange termijn niet. Slecht nieuws moet je snel brengen. Het wachten er mee of misschien helemaal niet melden zal ten koste gaan van het vertrouwen van gebruikers/klanten in de organisatie.

Weynand Haitjema, managing director EMEA van Pinkerton en Cees Siermann, managing partner Van Dantzig Communicatiepartners