CBP stelt minimale eisen databeveiliging vast

DEN HAAG - Het College bescherming persoonsgegevens (CBP) heeft een richtsnoer uitgebracht voor de beveiliging van informatie. Het document beschrijft waar de privacywaakhond op let bij onderzoeken om te toetsen of organisaties zich aan de wet houden.

Zo'n richtlijn is nodig, omdat beveiliging wettelijk verplicht is voor organisaties die persoonsgegevens verwerken. De wet is echter minder duidelijk over wat er precies moet worden gedaan. Zo eist de wetgever dat een organisatie 'passende technische en organisatorische maatregelen' moet nemen, rekening houdend met 'de stand van de techniek'.

Die onduidelijkheid in de wet leidt na cyberaanvallen vaak tot discussie of een bedrijf wel of niet voldoende aan beveiliging heeft gedaan. Wie privédata onvoldoende beveiligt riskeert ingrijpen van het CBP, waarbij in de toekomst mogelijk ook forse boetes kunnen worden opgelegd.

Risico-inschatting

Volgens het CBP moet daarom een beveiligingsplan worden opgesteld en moeten organisaties constant verbeteringen doorvoeren. Zo moeten het risico op een aanval worden ingeschat. Ook moet er een plan zijn voor het afdekken van de schade als een hacker toegang krijgt tot de informatie.

Ook moet worden ingeschat hoeveel privédata wordt verwerkt en hoe de privacy wordt beïnvloed als die data lekt. Dat hoeft niet altijd te leiden tot meer beveiligingsmaatregelen, maar zou ook als gevolg kunnen hebben dat er juist minder informatie wordt verwerkt. Zo neemt het risico immers ook af. Als gevoeligere informatie wordt verwerkt, moeten er strengere beveiligingsmaatregelen worden genomen. Gegevens die zwaar bewaakt moeten worden zijn bijzondere persoonsgegevens als medische informatie en details over ras, geloof en seksuele voorkeuren. Maar ook inloggegevens, financiële data en burgerservicenummers moeten beter worden beveiligd.

Standaarden

De richtlijn verwijst naar standaarden in de beveiligingsindustrie die de basis moeten vormen voor het beleid van organisaties. Zo wordt in de zorg de zogenoemde NEN-norm gehanteerd en bestaat er een Code voor Informatiebeveiliging voor het bedrijfsleven en de overheid. Die laatste standaard wordt nu op veel plekken nog niet gehaald. De richtlijnen voor webapplicaties en mobiele apparaten van het Nationaal Cyber Security Centrum (NCSC) worden door het CBP ook als voorbeelden van bestaande standaarden genoemd.

Bron: www.nu.nl Brenno de Winter d.d. 19-2-2013 (RIJ)