De visie van specialisten

‘Cyber security vergt een aanpak op wereldwijde schaal’

Bij het gebruik van websites en apps op onze computers, tablets of smartphones worden heel wat persoonlijke data opgeslagen. Security en privacy vormen dan ook een steeds grotere uitdaging in onze gedigitaliseerde maatschappij. ‘Het internet heeft geen grenzen’, zegt Chris Verdonck, partner en cyber leader bij Deloitte België. ‘Als gebruiker van online diensten of mobiele toestellen komen je gegevens daardoor – meestal onbewust – terecht op een wereldwijd platform. Je bent dus heel wat kwetsbaarder dan vroeger, toen je klantenkaart bewaard werd in een bakje onder de toonbank.’

De digitale nabijheid die het internet met zich meebrengt, creëert echter ook een heleboel opportuniteiten voor organisaties die hun business op een globale manier willen uitbreiden. Afstanden zijn verdwenen: bedrijven hebben vandaag toegang tot de hele wereld. Hoe groter de ‘digital proximity’, hoe groter de waarde van een internationaal opererende onderneming. Maar tegelijkertijd brengt die een heleboel verplichtingen met zich mee: de verzamelde data moeten op een correcte manier beheerst worden.

Zoektocht naar betere beveiliging

De snelheid waarmee de digitalisering onze wereld verovert, brengt extra uitdagingen met zich mee. In amper tien jaar tijd hebben smartphones en sociale netwerksites een belangrijke plek ingenomen in ons leven. Gebruikers, bedrijven en overheden worden nu geconfronteerd met security en privacy issues, maar ze kunnen niet terugvallen op een lange historiek of expertise om deze razendsnelle evolutie in goede banen te leiden. De zoektocht naar een betere beveiliging gebeurt dus met vallen en opstaan. Het feit dat er vanuit onze overheid pas heel recent concrete vragen gesteld worden over het privacybeleid van Facebook, is een voorbeeld.

Chris Verdonck, partner en cyber leader bij Deloitte België.

‘Het internet heeft geen grenzen. Ook niet voor malafide spelers.’

Ook de toegenomen toegankelijkheid van het internet maakt gebruikers extra kwetsbaar. ‘Nog niet zo heel lang geleden kon je alleen naar websites surfen met een computer’, illustreert Verdonck. ‘Daartoe moest je eerst inbellen via een telefoonlijn. Daarna kon je het internet opnieuw letterlijk ‘uitzetten’. Vandaag zijn zelfs onze kinderen via verschillende devices – denk aan de smartphone, Xbox, internettelevisie of wearables – permanent verbonden met het world wide web. De gevaren van deze ononderbroken ‘connectivity’ mogen niet onderschat worden.’

Wettelijk kader is nodig

Een wettelijk kader inzake de bescherming van gebruikersgegevens dringt zich sowieso op. Overheden dienen daarbij een beleid uit te werken op regionaal én internationaal niveau. Chris Verdonck: ‘Concrete maatregelen moeten genomen worden op grote schaal. Want de ‘digital proximity’ zorgt er ook voor dat malafide spelers overal aanwezig zijn. Een cyberattack is een heel virtueel gebeuren: een persoon op plaats A kan via een server op plaats B een bedrijf op plaats C aanvallen. Vergelijk het met het Ebolavirus: zo’n dreiging kan je alleen uitroeien via een gestructureerde, internationale aanpak.’

ZO BESCHERMT U UW ORGANISATIE

Organisaties bekijken cyberrisico’s vaak vanuit een louter technisch standpunt. Het is echter veel meer een business probleem. Deloitte Belgium ontwikkelde een methodologie die intussen wereldwijd toegepast wordt om de business tegen cyber te beschermen. Ze schrijft voor om eerst de relevante dreigingen voor de organisatie te bepalen, en na te gaan welke afdelingen kwetsbaar zijn voor welke cyberbedreigingen. Daarna wordt nagegaan in welke mate ze al opgewassen zijn tegen de specifieke cyberbedreigingen. Vervolgens wordt bepaald welke maatregelen op welke plaatsen moeten getroffen worden, en welke budgetten daarvoor nodig zijn. De resulterende dashboards leveren de bedrijfsleiders en de board een duidelijk zicht op de huidige situatie en laten toe om een roadmap met prioriteiten op te stellen.

‘De risico’s en actoren kunnen overigens verschillen naargelang de verschillende industrieën en zelfs business services binnen eenzelfde onderneming’, weet Chris Verdonck. ‘Neem nu een bank: een mogelijk gevaar bij internetbankieren is phishing, terwijl de risico’s bij geldafname aan een bankautomaat shoulder surfing en skimming zijn. Het komt er dus eens te meer op aan om de kwetsbaarheid van elk onderdeel van je organisatie in kaart te brengen en vervolgens de gepaste cyberstrategie te bepalen.’

Wenst u meer informatie over de campagne Tomorrow is Today?

*Surf dan naar **www.tomorrowistoday.be**. Volgende week leest u hier alles over Digital Smart Banking.*

Deloitte.