NIEUWS | *04 april 2016*

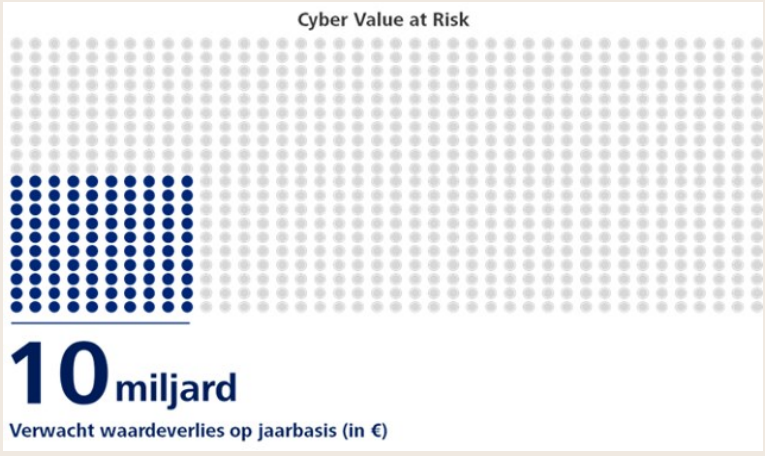
Deloitte: Cybercrime kost Nederlandse organisaties 10 miljard euro per jaar

Leestijd van ongeveer 4 minuten 0 reacties

Deloitte heeft voor het eerst de cyberrisico's in Nederland gedetailleerd en gekwantificeerd in beeld gebracht door middel van data analyse. Deloitte schat het totale waardeverlies door cyberrisico's voor de grootste Nederlandse bedrijven en overheid op jaarbasis op 10 miljard euro.

Echter, uitgaande van een worst-case scenario kan dit bedrag voor individuele organisaties oplopen tot achttien keer meer dan het waardeverlies dat ze mogen verwachten. Dit blijkt uit de data-analyse *Cyber Value at Risk in The Netherlands* dat Deloitte dat voorafgaand aan de International NCSC One Conference in Den Haag publiceert.

Het onderzoek werpt licht op zowel de gemiddelde impact van cyberrisico's als op de totale *Cyber Value at Risk*: het waardeverlies dat worst-case cyberincidenten kunnen veroorzaken voor de Nederlandse overheid en het bedrijfsleven. "Doel van het onderzoek is om organisaties inzicht te geven in het risico dat ze lopen op waardeverlies door cyberincidenten. Het geschatte waardeverlies van 10 miljard euro moeten we zien als *'costs of doing business'* door de digitalisering van onze samenleving. Dit brengt ons veel welvaart. Cybercrime is hier helaas onlosmakelijk aan verbonden, maar ook te managen. Op basis van onze data-analyse kunnen organisaties beter bepalen hoe ze hun businessmodel verder kunnen digitaliseren zonder te veel risico te lopen op het gebied van cybercriminaliteit," aldus Maarten van Wieren, cybersecurity expert bij Deloitte.



Cyberrisico's binnen Nederlandse sectoren

Het onderzoek richt zich op de meest relevante economische sectoren van Nederland. Uit de data-analyse blijkt dat als het gaat om cyberdreigingen, momenteel de volgende vier sectoren in verhouding tot hun omvang het grootste risico lopen: de publieke sector (totaal 2,4 miljard euro verwacht waardeverlies op jaarbasis), de technologie- & elektronicasector (1,1 miljard euro), de bankensector (360 miljoen euro) en de defensie-, luchtvaart- en ruimtevaartsector (415 miljoen euro).

LAATSTE NIEUWS

NIEUWS | *Gisteren*
Sports Direct in gesprek met MHA Macintyre Hudson

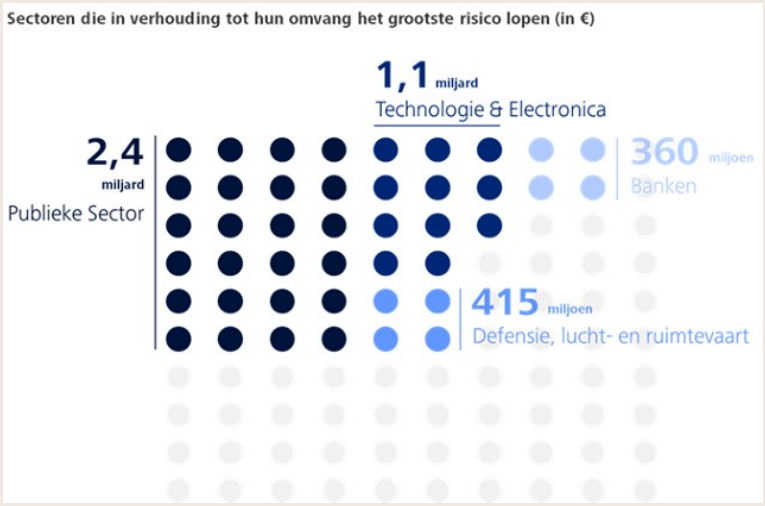
NIEUWS | *Gisteren*
Kamervragen over rol accountant bij misstanden Privazorg

NIEUWS | *Gisteren*
VEB schikt met voormalige bestuurders en commissarissen Innoconcepts

NIEUWS | *Gisteren*
'Arbeidsmarkt voor freelancers zwakt af'

NIEUWS | *Gisteren*
Rechtszaak tegen oprichter en topvrouw Oracle

MEER NIEUWS



Verschillende type cyberdreigingen

Het onderzoek neemt de verschillende soorten van misbruik van informatie door de verschillende cyberaanvallers als uitgangspunt. Zo blijkt dat een groot risico op waardeverlies (ruim 40 procent) voortkomt uit onderbrekingen van de operationele continuïteit. Dit is het gevolg van gerichte aanvallen door partijen die uit zijn op verstoring evenals een bijkomend gevolg van de breed-gerichte cybercriminaliteit. Dit raakt bijna alle organisaties.

Een ander groot waardeverlies (eveneens bijna 40 procent) komt voort uit verlies van intellectueel eigendom, strategische informatie en verminderde betrouwbaarheid van producten en diensten. Dit laatste verklaart een groot deel van het waardeverlies voor de publieke sector, de technologie- & elektronicasector en de defensie-, luchtvaart- en ruimtevaartsector. Voor de banken komt het grootste deel van het risico op dit moment voort uit de grote hoeveelheden vertrouwelijke informatie die ze over hun klanten hebben, terwijl hun risico om liquide middelen te verliezen relatief klein is.

Cyberweerbaarheid

Uit analyse blijkt verder dat hoe groter de organisatie des te volwassener het cybersecuritybeleid van de organisatie over het algemeen is. Ook de eerdere ervaringen met cyberdreigingen spelen een belangrijke rol. Zo blijken banken, de olie-, gas- en chemiesector, defensie-, lucht- en ruimtevaartsector evenals onderdelen van de centrale overheid relatief volwassen te zijn in hun cybersecurity. “Uit data blijkt dat hoewel de totale dreiging voor een sector hoog kan zijn, de impact van cyberincidenten flink omlaag gebracht kan worden met behulp van een goede cyberverdediging. Omdat cyberincidenten nooit helemaal te voorkomen zijn, is het van groot belang de negatieve impact zo veel mogelijk te beperken door goede detectie en snelle reactie,“ zegt Maarten van Wieren.

“Het is belangrijk om te beseffen dat het niet gaat om of je gehackt wordt, maar om wat je doet als je gehackt wordt. Geef cyberrisico’s daarom een aparte plek in je *operational risk framework*. Door te laten zien dat je controle hebt over je data, kan dit leiden tot vertrouwen en vertrouwen kan op haar beurt weer waarde toevoegen,” aldus Dick Berlijn, senior board advisor bij Deloitte.

Over het onderzoek

In 2011 introduceerde het World Economic Forum (WEF) het 'Risk & Responsibility in a Hyper-connected World'- initiatief. Samen met het WEF en met input van meer dan honderd internationale experts, zakelijke en politieke leiders op het gebied van cybersecurity, publiceerde Deloitte begin 2015 een rapport over *Cyber Risk Quantification*, waarbij voor het eerst het *Cyber Value at Risk*-concept geïntroduceerd werd.

Gezien het belang van cybersecurity voor onze samenleving besloot Deloitte om dit concept door te ontwikkelen. Op basis van het model is vastgesteld wat de kwantitatieve impact van cyberrisico's op organisaties binnen de meest relevante sectoren in Nederland is. Op basis hiervan kunnen Nederlandse bestuurders beter bepalen welke investeringen binnen hun organisatie wel of niet nodig zijn op het gebied van cybersecurity. De data-analyse is uitgevoerd binnen het State of the State-programma van Deloitte.

Dit is een actuele data-analyse van ons land, bedoeld om beleidsmakers en organisaties van bruikbare inzichten te voorzien op het gebied van maatschappelijke onderwerpen zoals veiligheid en cybersecurity. Deloitte analyseerde hiervoor voor het derde jaar op rij open data in onderlinge samenhang. Op www.stateofthestate.nl zijn deze nieuwe inzichten te vinden.

Reacties

Deel dit artikel

GERELATEERD

NIEUWS | *22 juli 2019*

Equifax schikt hack voor 700 miljoen dollar

Het Amerikaanse kredietbureau Equifax schikt een zaak rond een grote hack bij het bedrijf voor 700 miljoen dollar. Dat heeft de Amerikaanse toezichthouder Federal Trade Commission (FTC) bekendgemaakt. Daarmee komt een einde aan onderzoeken van de Amerikaanse federale overheid en een aantal staten. →

x 0

NIEUWS | *17 juli 2019*

CBS: '1,2 miljoen slachtoffers van digitale criminaliteit'

In 2018 gaf 8,5 procent van de internetgebruikers van 12 jaar of ouder aan in de afgelopen twaalf maanden slachtoffer te zijn geweest van digitale criminaliteit. Dat komt neer op ruim 1,2 miljoen mensen. →

x 0

NIEUWS | *13 mei 2019*

EU kan sancties opleggen aan cybercriminelen

De Europese Unie kan binnenkort sancties opleggen aan mensen of organisaties die betrokken zijn bij cyberaanvallen. De 28 lidstaten zijn maandag akkoord gegaan met zo'n strafsysteem waarmee banktegoeden kunnen worden bevroren en reisverboden opgelegd. Het wordt vrijdag officieel aangenomen. →

x 0

NIEUWS | *13 mei 2019*

Grote bedrijven pakken cybercrime samen aan

Grote bedrijven als ABN AMRO, Ahold Delhaize, Shell, IBM, ING en KPN slaan de handen ineen tegen digitale criminaliteit en vandalisme. ABN AMRO brengt maandag bedrijven uit verschillende sectoren bijeen om het over de uitwisseling van informatie te hebben. Daaronder zijn cyberveiligheidsdirecteuren van verschillende bedrijven alsook mkb'ers en studenten. →

x 0

NIEUWS | *09 mei 2019*

Cyberaanval op Wolters Kluwer

Informatieleverancier Wolters Kluwer is getroffen door een cyberaanval. In enkele platforms en applicaties is schadelijke software (malware) aangetroffen. →

x 0

Accountant is een uitgave van de Koninklijke Nederlandse Beroepsorganisatie van Accountants (NBA).

NBA

Artikelen
Fraude in praktijk
Kantoormanagement
Mkb
Opleiding
Privacy
Samenstellen
Statistical auditing
ICT
Kwaliteit en toezicht
Ondernemingsrecht
Overheid
Professioneel-kritische instelling
SBR
Subsidies
Integrated reporting
Lerend vermogen
Onderzoek en wetenschap
Pensioen
Publiek belang
Semi-publieke sector
Van de Helpdesk