

Beveiliging - een nieuwe mix van uitdagingen

In 2025 zullen naar schatting 80 miljard IoT-apparaten gegevens genereren en een schat aan inzichten opleveren. Al deze gegevens moeten verwerkt, opgeslagen en beschermd worden en beveiliging zal een steeds complexere uitdaging worden.
Bedrijven moeten niet alleen aan datavolume denken. Een opkomende mix van uitdagingen is ook belangrijk om te overwegen bij het beslissen over hoe systemen moeten ontworpen worden.

- **Het menselijk risico**
  Mensen zijn vaak de zwakke schakel in de beveiligingsketen. Het zullen vooral biometrische gegevens zijn die menselijke risico's verminderen, zoals het achterlaten van fysieke documenten in het openbaar vervoer, het verliezen van apparaten of het vergeten van wachtwoorden.

- **IoT en randapparatuurbeveiliging**
  In een wereld waar alles verbonden is, neemt het risico op datalekken beslist toe. Bedrijven moeten ervoor zorgen dat geavanceerde apparaten, zoals *wearables* (draagbare technologie) en koelkasten, geen toegang bieden tot hun systemen.

- **Flexibel werken**
  In een wereld waar werknemers flexibel, autonoom en samen willen werken, moet netwerkbeveiliging sterk, onopvallend en naadloos zijn. Werknemers zien meerfasige aanmeldingen als een rem op de productiviteit en verwachten dat alles onmiddellijk toegankelijk is. Nogmaals, biometrie zal de veilige verzelfstandiging van personeel ondersteunen.

- **Persoonlijke gegevens en naleving**
  In heel Europa beschermen burgers steeds meer hun persoonlijke gegevens en ze zijn zich bewust van hun ‘recht om te worden vergeten’. GDPR zal als dusdanig niet het laatste stuk wetgeving zijn dat complexe naleving vereist. Bedrijven zullen hun systemen en processen moeten aanpassen om zich aan de initiatieven op regeringsniveau te houden of om hoge boetes te vermijden.

Vooruitkijken - de kritieke ontwikkelingen in cybersecurity
De komende jaren zullen technologische ontwikkelingen grote implicaties hebben voor en een grote invloed hebben op de evolutie van veiligheid.

- **Cloudmigratie**
  Cloudtechnologie werd ooit als een documentback-up bezien, maar komt nu steeds vaker voor als een primaire facilitator. De beveiligingsmaatregelen die door de cloud worden aangeboden, zijn ontworpen met toonaangevende beveiligingsexpertise. Fysieke scheiding, een vermindering van kwetsbaarheden, verbeterde veerkracht en constante updates zullen allemaal helpen om het beveiligingsniveau van de server te verbeteren.

- **Continue beveiligingscontrole**
  Offensieve beveiliging wordt ingezet om systemen die op zoek zijn naar bedreigingen te doorzoeken. Met deze opkomende technologie zullen organisaties cyberdreigingen een stap voorblijven en hebben ze een real-time zichtbaarheid van het gebruik van elk apparaat.

- **Blockchain (Blokketen)**
  Eenvoudig omschreven is *blockchain* een uiterst gedetailleerde lijstinformatie, maar het biedt veel potentieel om de wereld te verbeteren. Door een ongelooflijk gedetailleerd beeld van toeleveringsketens op te bouwen, zal het internet overal worden afgesloten voor dubieuze en criminele activiteiten, en zelfs de bescherming van corrupte regimes ongedaan maken. Het gebruik ervan in fintech (financiële technologie) zal ook leiden tot financiële traceerbaarheid, waardoor een einde komt aan duistere transacties. Als zodanig belooft blockchain de gegevensbeveiliging en bankprotocollen te hervormen.

- **Cognitieve cyberbeveiliging**
  Een potentieel nadeel van big data is de aantrekkelijkheid ervan voor cybercriminelen. Aan de andere kant begeleidt het ook de strijd tegen hen. Big data laat een spoor achter, waardoor het voor beveiligingsanalisten, -architecten en alomtegenwoordige leerprogramma's veel eenvoudiger wordt om aanvallen te voorspellen en daders te identificeren voordat ze handelen.



Voor meer tips, download gratis het volledige rapport