Waarom de taak van de IT-manager de hoogste prioriteit heeft

Als IT-manager ligt de digitale transformatie van uw bedrijf in uw handen. De argumenten om digitalisering en de bijbehorende risico's de hoogste prioriteit te geven, wegen steeds zwaarder. Het is daarom essentieel dat u in staat gesteld wordt om uw werk goed te doen en dat er geen miljoenenschade voor nodig is, om het belang van investeringen en preventie duidelijk te maken.

"Een investering in een goed cyberprogramma is een investering in het merk."

Digitalisering bepaalt in toenemende mate hoe we ons werk doen. Bedrijven gaan vaker in de cloud werken, thuiswerken wordt normaler en in de nabije toekomst worden meer tastbare zaken op het internet aangesloten. Voor veel organisaties is het dan ook verleidelijk om vol op digitalisering in te zetten: om de concurrentie voor te blijven, zijn voortdurend snellere, slimmere en efficiëntere oplossingen nodig. Maar veiligheid wordt daardoor een steeds belangrijker speerpunt. We bespreken een aantal risico's waarvan bedrijven zich bewust moeten zijn.

Onzekerheid dwingt tot flexibiliteit

We leven in een tijd van grote onzekerheden. Er woedt een handelsoorlog tussen China en de Verenigde Staten, vanwege de coronacrisis gaan honderdduizenden banen verloren en er dreigt er een ongekende wereldwijde recessie. Het is nu belangrijker dan ooit om te anticiperen op de veranderingen en uw organisatie zo flexibel mogelijk in te richten. Dat heeft bijvoorbeeld gevolgen voor de manier waarop u de productie- en leverketen inricht en de snelheid waarmee u producten in en uit de markt kunt zetten en halen. Om mee te kunnen bewegingen met deze veranderingen is een flexibele IT-organisatie nodig.

De maatschappij verwacht steeds meer van u

Er zijn verschillende maatschappelijke debatten gaande die invloed uitoefenen op de wijze waarop bedrijven omgaan met hun werknemers, de omgeving en de planeet. Het is niet langer genoeg om goede producten te maken, waarde te creëren en winst te maken. Er wordt van bedrijven verwacht dat zij hun sociale standaarden behalen. Heeft uw organisatie bijvoorbeeld diversiteit en inclusiviteit hoog in het vaandel staan? Dan is het zaak dat uw digitale systemen afgestemd zijn op uw veranderende omstandigheden.

AON
Empower Results®

Efficiency versus ethiek

Technologie loopt meer dan ooit voor op de wet- en regelgeving. Zo zijn er HR-afdelingen die met behulp van artificial intelligence hun selectieprocedures optimaliseren. Dergelijke technologie verschaft ons grote voordelen, maar ethische discussies zijn hierover nog onvoldoende gevoerd. Het is raadzaam dit risico voortdurend in de gaten te houden, om te voorkomen dat de waarde die de technologie toevoegt botst met de ethische opvattingen die ten grondslag liggen aan onze samenleving.

Toegang tot de digitale omgeving

Externe partners krijgen steeds vaker toegang tot de digitale omgeving van bedrijven. Dat maakt organisaties kwetsbaar op het gebied van compliance en security. Sommige partners werken in interne systemen waarin gevoelige data liggen opgeslagen. Dat kan problemen met de AVG en andere wet- en regelgeving opleveren. Als het misgaat, leidt dat in het ergste geval tot een datalek. Dit gaat mogelijk gepaard met reputatieschade en boetes, die voor flinke financiële tegenvallers kunnen zorgen, naast de forensische en herstelkosten. Het is daarom noodzakelijk dat u heldere afspraken maakt met betrokken partijen over bevoegdheden en omgang met vertrouwelijke gegevens.

De gevaren van dataverwerking

Door de groeiende invloed van algoritmes wordt big data steeds bruikbaarder en daardoor ook waardevoller. U bent als IT-manager verantwoordelijk voor de veiligheid van data die uw bedrijf verzamelt en verwerkt. Het is daarbij verstandig altijd aan de toekomst te denken: hoe veilig is de data in de toekomst nog wanneer we deze met de kennis en techniek van nu opslaan? Dataveiligheid is dus een continu proces. Welke maatregelen neemt u om de veiligheid van uw data te kunnen blijven waarborgen?

Significante toename van cyberincidenten

Tot slot is er een significante toename te zien van cyberincidenten. Enerzijds komt dat doordat cybercriminelen niet gehinderd worden door wettelijke en procesmatige beperkingen, waardoor ze IT-professionals vaak een stap voor zijn. Anderzijds hebben bedrijven hun detectie- en responsecapaciteit ondanks massale investeringen onvoldoende op orde. Als u wilt voorkomen dat u slachtoffer wordt van een cyberincident, dient cyberveiligheid bij uw organisatie hoog op de agenda te staan.

Aan de slag met de digitale transformatie?

Wilt u de digitale transformatie van uw bedrijf veilig laten verlopen? Aon's specialisten helpen u in elke fase van het proces met advies op maat.

Wij helpen u graag succesvol te ondernemen.

Ralf Willems
Aon Cyber Solutions
ralf.willems@aon.nl
+31 (0)10 448 77 72

Empower Results®

20.081-01-AW/IT Manager-01