Voorkom noodsprongen in de toekomst

'Een assessment van Salomon die korte termijn IT-oplossingen op de lange termijn in jouw voordeel laat werken'

Waarom dit assessment

- In kaart brengen welke adhoc acties er zijn ingezet en de impact hiervan duiden
- Optimaliseren van de IT-middelen die je nu hebt aangeschaft/ingezet
- Plan maken om toekomstige noodsituaties sneller en volgens beleid onder controle te krijgen

Welke stappen doorlopen wij:

1

Bedrijfsprocessen en beleid

Welke processen zijn er cruciaal binnen een organisatie en wanneer moeten deze beschikbaar zijn? Denk bijvoorbeeld aan het on- en offboarden van komend en vertrekkend personeel. De bedrijfsmiddelen die daarvoor moeten worden ingericht of teruggehaald. Maar ook de Salarisadministratie. Hoe is dit nu op afstand ingericht en hoe wordt de continuiteit daarvan gewaarborgd? Zijn daar nog externe partners bij betrokken en hoe benaderen zij nu jouw gevoelige data?

2

Collaboratiemiddelen en gebruik

Er wordt gekeken naar de middelen die zijn ingezet om digitaal vergaderen en samenwerken mogelijk te maken. Denk hierbij aan oplossingen als Microsoft Teams, Zoom, Google Hangouts e.d. Er wordt gecontroleerd of de gekozen oplossing in lijn is met het huidige beleid en eventuele AVG richtlijnen. Tevens wordt onderzocht of de software wel optimaal gebruikt wordt. Is alle functionaliteit duidelijk? Betaal je niet teveel aan licenties en benut je niet te weinig van het pakket? Zijn de gebruikers voldoende 'opgeleid' om de software effectief en efficiënt in te kunnen zetten?

3

De Thuiswerkplek en centrale infrastructuur

Welk type werkplek (hardware) mag de gebruiker thuis gebruiken? Is dit BYOD (Bring Your Own Device) of is er door het bedrijf een apparaat aangeschaft en uitgereikt? Welke gebruikers zitten daar thuis allemaal op te werken (partners en kinderen) en welke risico's brengt dit met zich mee? Hoe wordt er verbonden met de centrale werkomgeving? Wordt hier wel de juiste security afgedwongen? Denk hierbij aan VPN, Two Factor authentication e.d. Maar ook, hoe is de werkplek zelf beveiligd? Welke Antivirus/Spam oplossing is er actief? Is er een centrale aansturing van de verbonden clients ingeregeld? Hoe voorkom je digitale inbraak en waarborg je de integriteit van de data? Welk beleid is er hier van toepassing?

4

Korte versus lange termijn

Hoe zorg je ervoor dat de stappen die nu noodgedwongen zijn gezet passen bij de strategie en het beleid van de organisatie? Waar zijn eventuele aanpassingen noodzakelijk en hoe gaan we hier in de toekomst mee om? Hoe minimaliseer je de bedrijfsrisico's en hoe borgen we dat we bij een volgend crisisscenario meer controle kunnen uitoefenen? Lessons learned, mits hier op gepaste wijze mee wordt omgegaan maken je futureproof.

salomon IT

Welk inzichten levert dit je op:

1. Welke producten worden er gebruikt en voldoen die aan de gestelde AVG regelgeving en het bedrijfsbeleid
2. Weet men voldoende om te gaan met de in gebruik genomen producten (Teams, SharePoint, Zoom e.d.) of is er training nodig
3. Maakt de organisatie optimaal gebruik van de functionaliteiten die er binnen de aangeschafte licentievorm beschikbaar zijn
4. Welke producten of oplossingen kun je mogelijk als alternatief gebruiken of als 2e scenario indien de A-keuze niet langer een mogelijkheid is
5. Welke thuiswerkplekken, inclusief eventuele randapparatuur zijn er momenteel in gebruik, zijn deze veilig en waar zitten de risico's
6. Is de bedrijfsdata voldoende afgeschermd van risico's en hoe wordt de integriteit hiervan bewaakt
7. Welke top 5 maatregelen zijn er te treffen om een éénduidig beleid van security en controle af te dwingen, laten we dit de quick wins noemen
8. Is de eindgebruiker voldoende bewust van de risico's op het gebied van C-level fraude of Ransomware en Malware
9. Welke maatregelen zijn er te treffen om de organisatie controle te geven over werkplekken van werknemers die je niet meer dagelijks ziet
10. Welke kritische bedrijfsprocessen zijn er en welke zijn van belang om de continuïteit van een organisatie te waarborgen. En, welke technieken (resources) zijn er nodig om deze te ondersteunen
11. Welke van de geïmplementeerde technologieën of producten kan de organisatie blijvend gebruiken
12. Voldoet ons beleid nog of moet deze worden aangepast aan de toekomst

Wat kun je hier vervolgens mee?

1. Maatregelen treffen om ten tijde van toekomstige crisisscenario's adequaat en snel te kunnen handelen
2. Korte termijn oplossingen blijvend integreren volgens het beleid van de organisatie
3. Optimaliseren van geïmplementeerde/aangeschafte technische oplossingen
4. Huidige geïmplementeerde oplossingen afzetten tegen mogelijke alternatieven
5. Controle krijgen over de veiligheid van het thuiswerken
6. Thuiswerkers voorzien van kennis en kunde om volgens bedrijfsbeleid hun werkzaamheden uit te voeren
7. Inzichtelijk maken wanneer er welke bedrijfsprocessen voorrang moeten krijgen over andere en welke techniek er dan cruciaal is
8. Inzichtelijke stappen in waar het beleid van een organisatie moet veranderen om de toekomst tegemoet te komen
9. Gevoelige bedrijfsdata kan beter worden afgeschermd
10. Thuiswerken, ook na deze noodsituatie, blijvend en volgens eisen en wensen mogelijk houden

Meer informatie

Wilt u meer weten over dit assessment en onze dienstverlening?
Neem contact ons op via **0611583323** of **info@salomon.nl**

salomon.IT