

8 VRAGEN

die een IT Manager moet stellen bij het beoordelen van communicatietools

In de digitale wereld van vandaag, waarin op afstand werken de nieuwe norm is, vindt steeds meer communicatie plaats via digitale tools. Bij die communicatie wordt vaak zeer gevoelige bedrijfsinformatie gedeeld. Het spreekt voor zich dat deze tools gegarandeerd 100 procent veilig en gemakkelijk in het gebruik zijn. Personen die verantwoordelijk zijn voor het implementeren van en toezicht houden op het informatiebeveiligingsbeleid binnen een organisatie moeten verschillende communicatietools zorgvuldig en secuur beoordelen op functionaliteit, de mogelijkheid om samen te werken en uiteraard de beveiligingsinfrastructuur. IT Managers moeten in ieder geval de volgende acht vragen stellen aan aanbieders van communicatietools.

1. Investeert de aanbieder in onderzoek naar en ontwikkeling van cybersecurity?

Door de technologische vooruitgang en de winstgevendheid zijn cybercriminelen continu in ontwikkeling. Nu veel werknemers vanuit huis werken zijn er nog meer mogelijkheden ontstaan voor cybercriminaliteit. Hackers zijn inmiddels binnengedrongen in systemen van grote multinationals. Een betrouwbare aanbieder van beveiligde communicatietools moet in deze disruptieve tijd aantonen hoe zij anticiperen op de almaar grotere digitale dreiging van cybercriminelen. Hoe en in welke mate onderzoeken zij cybercriminaliteit en hoe is hun beveiliging hierop toegerust?

2. Is de aanbieder transparant over beveiligingsprocessen?

De aanbieder moet een duidelijke uitleg kunnen geven welke specifieke beveiligingsmaatregelen zij aanbieden. Denk hierbij aan de beveiliging van servers en andere apparatuur, de firewalls, de screeningsprocessen voor nieuwe medewerkers, de interne controles en de systeemmonitoring. Vraag ook om het beveiligingsplan voor incidenten. Hoe weet de aanbieder of er een hacker is doorgedrongen binnen het systeem? Ook is het van belang dat de aanbieder transparant is over eerdere inbreuken en hoe zij daarop heeft gereageerd. Al met al moet de aanbieder een goede staat van beveiliging kunnen aantonen en over de juiste beveiligingsprotocollen beschikken.

3. Voldoet de aanbieder aan de hoogste branchenormen?

Als externe verwerkers van vertrouwelijke gegevens moeten aanbieders van beveiligde communicatietools voldoen aan de hoogste beveiligingsnormen. Belangrijke certificeringen zijn: goede prestaties op het gebied van de jaarlijkse SOC-2/SSAE 18-audits en ISO 27001-certificering voor beveiliging. De beheersystemen voor informatiebeveiliging van de softwareleverancier moeten voldoen aan internationale normen.

4. Staat de aanbieder externe pentesten toe?

De meeste aanbieders van communicatietools voeren pentesten uit als onderdeel van hun kwaliteitscontrole. Goede softwareleveranciers die hoge beveiligingsnormen hanteren, voeren continu testen uit in plaats van jaarlijks en kunnen daardoor tijdig inspelen op acute dreigingen.

Aanbieders van communicatietools moeten hun klanten en potentiële klanten toestaan om onafhankelijke beveiligings- en pentests uit te voeren (zelf of door een zelf gekozen externe partij).

5. Welke vormen van fysieke beveiliging heeft de aanbieder geïmplementeerd?

Digitale gegevens worden opgeslagen op fysieke apparaten op fysieke plaatsen. De faciliteiten voor datahosting moeten zijn beveiligd met bewaking ter plaatse, beveiligingscamera's en meerdere niveaus van omgevingsbeveiliging. De servers zelf moeten worden geplaatst in beveiligde ruimtes waarbij de gehoste gegevens van alle organisaties gescheiden zijn. Cryptografische sleutels moeten worden bewaard op beveiligde apparaten die bestand zijn tegen hackers.

6. Welk niveau van gegevensredundantie wordt geboden?

Worden er back-ups van gegevens gemaakt en schakelen primaire datacentra na noodgevallen over naar een secundair datacentrum voor herstel? Aanbieders van beveiligde communicatietools moeten beschikken over meerdere afgelegen, verspreide locaties zodat een incident die de ene locatie treft, niet ook voor problemen zorgt op de secundaire locatie. Daarnaast moet gegevensredundantie 24/7 worden ondersteund door realtime inzicht in de prestaties.

7. Biedt de aanbieder de mogelijkheid om het beveiligingsniveau van het platform aan te passen aan uw situatie?

Iedere organisatie is uniek. Er bestaat niet één ideale beveiligingsoplossing voor alle organisaties. Een goed platform voor beveiligde communicatie biedt mogelijkheden om de functionaliteit af te stemmen op de specifieke beveiligingsbehoeften van een organisatie. Denk aan verschillende wachtwoordsterktes, een afwijkend vergrendelingsbeleid en de mogelijkheid om informatie te delen en er met meerdere mensen aan te kunnen werken.

8. Is er een goede klantsupport?

Het maakt niet uit hoe krachtig de beveiliging van een platform is, er is altijd menselijke ondersteuning nodig om ervoor te zorgen dat problemen snel worden opgelost. Als een bestuurslid bijvoorbeeld een paar keer het verkeerde wachtwoord invult en geen toegang tot het systeem meer heeft, moet deze onmiddellijk een telefoontje van de klantsupport ontvangen. Dit is niet alleen noodzakelijk om directe hulp te bieden, maar ook om de oorzaak van de mislukte pogingen te controleren.

Over Diligent

Diligent is leider in Modern Governance. Met onze middelen en technologie bieden wij bestuurders en directieleden het inzicht om zo goed en efficiënt mogelijk te besturen. Zij beschikken over de juiste informatie om altijd de juiste beslissingen te kunnen nemen. Zo vermijden ze een 'governance deficit' waarbij ze te laat te weinig informatie krijgen.

Meer dan 17.000 organisaties en 700.000 gebruikers in meer dan 90 landen vertrouwen op Diligent. De bekroonde klantenservice van Diligent zet zich wereldwijd in en ondersteunt meer dan 50% van de Fortune 1000-bedrijven, 65% van de AEX-bedrijven en 52% van de BEL20-bedrijven.

Kom meer te weten over de beveiligde samenwerkingstools van Diligent:

De oplossingen van Diligent bieden ondernemers en bestuurders beveiligde alternatieven voor e-mail en de mogelijkheid om samen te werken aan uiterst gevoelige documenten en workflows.

Benieuwd naar hoe de tools voor uw organisatie werken?

DEMO AANVRAGEN

Neem voor meer informatie of het aanvragen van een demo vandaag nog contact met ons op:

E-mailadres: info@diligent.com
Telefoon: Nederland +31 (0) 20 299 6769

België +32 (0) 929 80 423
Website: www.diligent.com/nl