Diligent

8 VRAGEN

die een CISO moet stellen bij het beoordelen van oplossingen voor beveiligde communicatie

Nu organisaties noodgedwongen moeten omschakelen en thuiswerken, zagen CISO's de behoefte aan oplossingen voor beveiligde communicatie ter ondersteuning van de bedrijfscontinuïteit snel toenemen. In deze nieuwe, digitale wereld moeten organisaties hun meest gevoelige documenten en bedrijfsinformatie toevertrouwen aan digitale tools. Zulke tools moeten uiteraard zorgvuldig worden beoordeeld op functionaliteit, samenwerkingsmogelijkheden en de beveiligingsinfrastructuur. Personen die verantwoordelijk zijn voor de technologie en de beveiligingsinfrastructuur moeten een software selecteren die betere communicatie ondersteunt. Voor nu en in de toekomst. Daarnaast moeten ze ervoor zorgen dat de bestuursleden, de company secretary en executives, de general counsels en het managementteam goed kunnen omgaan met deze tools. Tot slot moeten ze vertrouwen hebben in de beveiliging, zodat cruciale taken en processen kunnen worden voortgezet.

We hebben de 8 vragen opgesteld die uw organisatie moet stellen aan potentiële aanbieders van beveiligde communicatie:

1 Investeert de aanbieder aanzienlijk in het onderzoek en de ontwikkeling van cyberbeveiliging?

Door de technologische vooruitgang en de winstgevendheid van de cyberonderwereld zijn cyberdreigingen continu in ontwikkeling. Nu velen vanuit huis werken zijn er nog meer unieke mogelijkheden ontstaan voor cybercriminelen. Hackers hebben zich weten binnen te dringen in ontwikkelde organisaties en hebben daarmee disruptie op wereldwijde schaal veroorzaakt. Een betrouwbare aanbieder van beveiligde communicatie kan aantonen welke mogelijkheden tot onderzoek en ontwikkeling deze heeft om opkomende dreigingen voor te blijven.

2 Is de aanbieder transparant over beveiligingsprocessen?

De aanbieder moet een duidelijke uitleg kunnen geven over de fysieke en logische beveiligingsmaatregelen (beveiliging van servers, toepassingen, firewalls en andere apparatuur), de screeningsprocessen voor nieuwe medewerkers, de interne controles, de systeemmonitoring, het reactieplan voor incidenten (hoe weet de aanbieder of er een hacker is doorgedrongen?) en de geschiedenis van eerdere inbreuken plus de aanpak daarvan. Als de aanbieder een goede staat van beveiliging kan aantonen en over de juiste beveiligingsprotocollen beschikt zorgt dat voor geruststelling.

Diligent

3 Voldoet de aanbieder aan de hoogste branchenormen?

Als externe verwerkers van vertrouwelijke gegevens moeten aanbieders van beveiligde communicatie voldoen aan de hoogste beveiligingsnormen, die vergelijkbaar zijn met die van andere IT-afdelingen in verschillende branches. 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 de internationale normen).

4 Staat de aanbieder externe pentesten toe?

De meeste aanbieders van beveiligde communicatie technologie voeren pentesten uit als onderdeel van hun kwaliteitscontrole. Goede softwareleveranciers die hoge beveiligingsnormen hanteren, voeren zelfs bijna continu tests uit in plaats van jaarlijks en kunnen daardoor tijdig inspelen op opkomende dreigingen. Ze moeten hun klanten en potentiële klanten toestaan om onafhankelijke beveiligings- en pentests uit te voeren (zelf of door een zelf gekozen externe partij). Aanbieders tonen op deze manier niet alleen het vertrouwen in hun oplossing, maar erkennen zo tegelijkertijd dat beveiliging een teamprestatie is.

5 Welke vormen van fysieke beveiliging heeft de aanbieder geïmplementeerd?

Hoewel we digitale gegevens vaak als iets ontastbaars beschouwen, worden deze wel opgeslagen op tastbare middelen. Deze faciliteiten voor datahosting moeten worden beveiligd met bewaking ter plaatse, beveiligingscamera's en meerdere lagen 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 datacenters indien nodig over naar datacenters voor herstel na noodgevallen? Aanbieders van beveiligde communicatie moeten beschikken over meerdere afgelegen, verspreide locaties zodat een gebeurtenis die de ene locatie beïnvloedt, 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?

Elke beveiligingsoplossing brengt een compromis tussen gemak en beveiliging met zich mee. Er is dus niet één ideale oplossing voor alle organisaties. Een goed platform voor beveiligde communicatie biedt mogelijkheden om de functionaliteit af te stemmen op de specifieke beveiligingsbehoeften van de organisatie. Denk bijvoorbeeld aan verschillende wachtwoordsterktes, vergrendelingsbeleid en opties om materialen te delen en er samen aan te werken.

8 Is er klant support beschikbaar?

Het maakt niet uit hoe krachtig de beveiliging van een platform is, er is altijd menselijke monitoring 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 klant support ontvangen. Dit is niet alleen noodzakelijk om hulp te bieden, maar ook om de oorzaak van de mislukte pogingen te controleren.

Diligent

Over Diligent

Diligent is leider in Modern Governance. Met onze middelen en technologie bieden wij ondernemers en bestuurders 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. Dat is Modern Governance. Meer dan 16.000 organisaties en 650.000 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

Download in de App Store | Downloaden van Microsoft | ONTDEK HET OP Google Play | AICPA SOC | ISO 27001 CERTIFIED BY BRIGHTLINE

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