

Is onze beveiliging op orde?

5 vragen die u moet stellen over de communicatie van bestuursleden en executives



De communicatie van bestuursleden en managementteams vereist een hoog niveau van beveiliging. Zij zijn namelijk interessante doelwitten voor hackers omdat ze toegang hebben tot belangrijke en gevoelige gegevens. In een recente enquête van Forrester en Diligent gaf meer dan de helft van de bestuurders en senior managers aan regelmatig een persoonlijk e-mailadres te gebruiken om te communiceren over gevoelige onderwerpen. Daarmee stellen ze de gegevens van hun bedrijven bloot aan aanzienlijke risico's.

Met een oplossing voor beveiligde communicatie kunt u de controle houden. Bovendien kunt u de tool gebruiken om documenten en bestanden snel en eenvoudig te delen en om snel te reageren tijdens crises. Maar niet alle oplossingen zijn gelijkwaardig. Houd rekening met het volgende als u de opties gaat evalueren:



1. Is de communicatie versleuteld?

Bij versleuteling wordt gewone tekst omgezet in een cryptografische sleutel: een reeks tekens om informatie te beschermen wanneer deze wordt overgedragen. Versleuteling is de effectiefste methode om gegevens te beveiligen en is een essentieel onderdeel van elke communicatieoplossing. Waarom? Omdat gevoelige gegevens die worden overgedragen, kwetsbaar zijn voor phishing-aanvallen, wachtwoordhacks en andere mogelijke inbreuken.

Uw communicatieoplossing moet berichten en bijlagen beveiligen met een moderne beveiligingsinfrastructuur en versleuteling. De ISO 27001-certificering is de gouden standaard voor informatiebeveiliging.

Andere essentiële functies: de mogelijkheid om berichten in te trekken en alleen-weergeven bijlagen te sturen. Met de laatste optie voorkomt u dat bijlagen worden gedownload, opgeslagen, geëxporteerd, gefotografeerd als schermafbeelding, gekopieerd of doorgestuurd naar andere gebruikers.



2. Zijn de platforms geïntegreerd?

Als gevoelige gegevens op verschillende plekken worden bewaard (bijvoorbeeld in e-mails, op apparaten van bestuurders en in verschillende systemen), neemt de kans op beveiligingsproblemen toe. Een communicatieoplossing met berichten, chat, samenwerking, gegevensopslag en meer via één platform biedt veel voordelen voor bestuurders en executives.

Organisaties doen er goed aan oplossingen te overwegen die het beveiligde berichtenplatform koppelen aan systemen voor het beheren, opslaan en delen van documenten. Zodat onbeveiligde kanalen als e-mail overbodig zijn.



3. Kunt u de oplossing gemakkelijk implementeren en gebruiken?

Bijna de helft (49%) van de respondenten heeft in de enquête van Diligent aangegeven dat het beveiligen van documenten of bestuursmaterialen 'uitdagend' of 'zeer uitdagend' is.

Om te garanderen dat bestuurders de oplossing gebruiken (en gegevens dus worden beveiligd), moet de communicatieoplossing aan de volgende vereisten voldoen:

- ☐ De functionaliteit en het ontwerp komen overeen met die van alledaagse tools en systemen (zoals e-mail en sms).
- ☐ De oplossing biedt mogelijkheid tot realtime updates en meldingen.
- ☐ De oplossing ondersteunt communicatie tussen allerlei groepen (zoals peer-to-peer, commissies, het gehele bestuur of het team van executives).



4. Worden de risico's beperkt?

Bijna een derde (29%) van de door Diligent ondervraagde bestuursleden is in het afgelopen jaar weleens een apparaat kwijtgeraakt. Daarnaast heeft 21% aangegeven dat de identiteit van iemand binnen het bestuur werd gestolen en gebruikt voor toegang tot betrouwbare materialen.

Één incident kan onherstelbare schade en financiële problemen veroorzaken. Zorg er daarom voor dat uw communicatieoplossing:

- ☐ Beheerders de mogelijkheid biedt om kwijtgeraakte of mogelijk gecompromitteerde apparaten op afstand te wissen.
- ☐ Wordt ondersteund door trainingen over productgebruik en cybermaatregelen.



5. Voldoet de oplossing aan de normen van uw beveiligingsteam?

Betrek het IT-team actief bij het selectieproces voor een oplossing, zodat gevoelige gegevens worden beveiligd en uw organisatie wordt beschermd tegen onnodige risico's.

CIO's en CISO's willen het volgende weten over een oplossing voor beveiligde communicatie:

- ❑ **Toegang en rechten:** In welke mate hebben beheerders controle over toegangsrechten en -locaties? Kunnen ze bijvoorbeeld toegang voor bepaalde gebruikers beperken of uitschakelen en kunnen ze voorkomen dat mensen toegang krijgen vanaf onbekende apparaten?
- ❑ **Vindbaarheid:** Hoe worden berichten bewaard en verwijderd? Bestaat de mogelijkheid om rapporten te maken over berichten die in een specifieke periode zijn verstuurd?
- ❑ **Redundantie:** Wordt er een back-up van gegevens gemaakt op verschillende afgelegen, verspreide locaties? Biedt de aanbieder 24/7 inzichten in alle gegevens?
- ❑ **Aanpassingsmogelijkheden:** Kan de oplossing worden afgestemd op de behoeften van het bestuur, bijvoorbeeld wat betreft wachtwoordsterkte en vergrendelingsbeleid?

CIO's en CISO's willen ook weten of de aanbieder van de oplossing:

- ❑ Investeert in onderzoek en ontwikkeling op het gebied van cyberbeveiliging.
- ❑ Open is over beveiligingsprocessen zoals systeemmonitoring, inbreuken en oplossingen, beveiliging van servers en routers en screening van nieuwe medewerkers.
- ❑ Regelmatig pentests uitvoert om snel te kunnen inspelen op opkomende dreigingen.
- ❑ Training en klantenondersteuning biedt, bijvoorbeeld om een bestuurslid te helpen die meerdere keren het verkeerde wachtwoord heeft ingevoerd en nu geen toegang meer heeft tot het systeem.

Tools van Diligent voor beveiligde samenwerking:

- ▶ **Diligent Boards:** biedt een beveiligde en centrale locatie voor vergadermappen en gevoelige vergadermaterialen, evenals tools voor revisie, discussie en samenwerking. Met deze app kunt u ook stemmingen regelen en vragenlijsten laten invullen.
- ▶ **Diligent Messenger:** een beveiligd, versleuteld berichtenplatform (op telefoon, iPad en desktop) dat vergelijkbaar is met sms en e-mail. Hiermee biedt u besturen en senior managementteams de mogelijkheid om veilig in groepen of een-op-een te communiceren. Messenger kan worden geïntegreerd met Diligent Boards.
- ▶ **Secure File Sharing:** een virtuele dataroom die kan worden geïntegreerd met Diligent Boards. Ideaal voor fusies en overnames, crisiscommunicatie of het delen van gevoelige documenten met gemachtigde externe partijen (zoals auditors en adviseurs).
- ▶ **Secure Meeting Workflow:** een workflowtool waarmee gemachtigde gebruikers kunnen samenwerken aan documenten en presentaties in een beveiligde, versleutelde omgeving.



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