



Het belang van het gebruik van beveiligde communicatietechnologie in de bestuurskamer

De voordelen van de Diligent Messenger-module

Communicatie tussen bestuurders en beheerders is essentieel voor een effectief en efficiënt bestuur. Het is alarmerend dat executives en bestuurders vertrouwelijke informatie verzenden naar de privé-e-mailaccounts van bestuurders: deze accounts zijn onvoldoende beveiligd en kwetsbaar voor gegevensdiefstal. E-mail blijft zeer kwetsbaar voor aanvallen. Volgens het rapport¹ Symantec ISTR Email Threats 2017 worden ongeveer 8000 bedrijven elke maand bestookt met zakelijke e-mails die in werkelijkheid scams zijn. E-mail en andere communicatiemiddelen zijn ook kwetsbaar voor phishing-aanvallen, wachtwoordhacks en andere mogelijke gegevensschendingen.

Uw gevoelige bestuursinformatie moet veilig blijven. Als u dus nog e-mail en sms gebruikt om bestuursgerelateerde materialen te verzenden, brengt u het bestuur en uw hele organisatie in gevaar.

Als marktleider in draagbare technologie voor de besturen, heeft Diligent een unieke positie om strategische en bruikbare inzichten te bieden over het snel veranderende digitale landschap. In dit rapport onderzoeken we de risico's van het gebruik van onveilige e-mail en communicatiemiddelen, bespreken we de voordelen van beveiligde communicatietechnologie voor besturen en houden we een pleidooi voor het gebruik van Diligent Messenger, een beveiligd communicatiemiddel dat speciaal is ontwikkeld voor de bestuurskamer.



Diligent

UITDAGINGEN EN RISICO'S

E-mail is niet veilig

Bestuurders verzenden bestuursmaterialen per e-mail omdat ze dit eenvoudig en handig vinden. Sommige bestuurders gebruiken zelfs privé-e-mail. Uit het rapport van NYSE Governance Series/Diligent² blijkt dat 60% van de bestuurders regelmatig privé-e-mail gebruikt om te communiceren met medebestuurders en het uitvoerend management. Het gebruik van e-mail, vooral privé-e-mail, voor het verzenden van bestuursmaterialen is echter risicovol. Niet alle communicatieoplossingen van andere leveranciers hebben hetzelfde beveiligingsniveau als Diligent. Privé-e-mails, bijvoorbeeld accounts bij Yahoo! en Gmail, staan op een open en gedeeld platform. Elke e-mailgebruiker kan bedoeld of onbedoeld vertrouwelijke informatie doorsturen naar onbevoegde gebruikers. Helaas zijn hackers ook op de hoogte van deze kwetsbaarheden. Problemen met e-mailaccounts van hooggeplaatste personen, zoals de voormalige Amerikaanse ministers van Buitenlandse zaken Hillary Clinton en Colin Powell, zijn volop in het nieuws geweest.

Aanvallers richten zich op het bestuur

Informatie uit het bestuur en communicatie tussen bedrijfsexecutives, company secretaries en bestuurders zijn vaak zeer gevoelig. Wanneer bestuurders privé-e-mailaccounts mogen gebruiken, vormt dit een risico voor zowel de bestuurders en bedrijfsmanagers als de hele organisatie. Als informatie wordt gelekt en openbaar wordt gemaakt, kan dit in sommige gevallen rampzalige gevolgen hebben voor het bedrijf (juridische consequenties, bekendwording van bedrijfsgeheimen, impact op inkomsten, schade aan merknaam).

Criminelen, hackers en kwaadwillende concurrenten kennen deze kwetsbaarheid en richten hun aanvallen op bestuurders, die als belangrijke doelen worden beschouwd. 'Phishing' is een e-maildreiging waarbij e-mails worden verzonden die afkomstig lijken te zijn van betrouwbare bedrijven en waarin slachtoffers worden overgehaald om gevoelige informatie te verstrekken. Deze frauduleuze praktijk is getransformeerd tot een geavanceerdere vorm die bekendstaat als "whaling". In 2016 werd ingebroken op het e-mailaccount van Colin Powell en werd vertrouwelijke informatie bekendgemaakt, waaronder informatie over geplande fusies en overnames van Salesforce, waar Powell toen bestuurslid was.³

E-mail is rommelig

De snelheid en het volume van e-mail vormen geen beveiligingsdreiging, maar kunnen wel een belemmering vormen voor effectieve communicatie tussen de bestuurders. Sommige bestuurders zitten in verschillende besturen en werken bij verschillende organisaties. Ze worden vaak bedolven onder bergen e-mails. Bestuursleden zijn vaak betrokken bij operationele processen, zoals goedkeuring van leningen, uitkering van verzekeringen en uitbetaling van pensioenfondsen. Door rommelige e-mail kunnen deze processen vertraging oplopen. Hoe kunnen bestuurders bestuursgerelateerde berichten herkennen en tijdig afhandelen tijdens het uitvoeren van deze verschillende taken en het verwerken van e-mails?



HOE DILIGENT MESSENGER KAN HELPEN

Besturen moeten proactief zijn op het gebied van beveiliging, maar waar moeten ze beginnen met technologie voor beveiligde bestuurscommunicatie? Niet alle aanbieders van communicatietechnologie zijn dezelfde. Sommige communicatiemiddelen bieden niet de strenge beveiliging die nodig is voor het bestrijden van geavanceerde dreigingen en andere bieden specifieke functies niet, waardoor er meer problemen kunnen ontstaan.

Diligent Messenger kan naadloos worden geïntegreerd met Diligent Boards en biedt specifieke oplossingen voor de uitdagingen en risico's waarmee besturen te kampen hebben bij onbeveiligde e-mail en sms.

Laten we enkele kenmerken en voordelen van Diligent Messenger bekijken:

Geavanceerde beveiligingstechnologie

Diligent Messenger is uitgerust met krachtige versleutelingstechnologie en maakt gebruik van dezelfde beveiligingsstandaarden als Diligent Boards. Diligent is ISO 27001-gecertificeerd, waardoor organisaties erop kunnen vertrouwen dat ze samenwerken met een aanbieder van beveiligde communicatietechnologie met een bewezen staat van dienst.

In tegenstelling tot privé-e-mail of e-mail van derden, biedt Diligent Messenger een gesloten omgeving met alleen bevoegde en goedgekeurde gebruikers. Alle informatie staat dus binnen de beveiligde Diligent-omgeving. Als iemand een apparaat verliest of als een apparaat wordt gehackt, kan het gebruikersaccount snel worden uitgeschakeld om gegevensdiefstal te voorkomen. Bovendien kan binnen de Messenger-omgeving niets worden ontdekt. Bestuurders en gebruikers kunnen het systeem met vertrouwen gebruiken en er zeker van zijn dat tijdens een audit geen van hun berichten kan worden gelezen of gevonden.

Diligent voert regelmatig controles uit van zijn beveiligingstechnologie, waaronder:

- **Jaarlijkse SSAE 16/ISAE 3402 (SOC 1 type 2)-audit door een externe dienstverlener**
- **SOC 2-audit van type 2 betreffende beveiliging en beschikbaarheid**
- **HIPAA AT 101-audit**
- **ISO 27001-gecertificeerd sinds februari 2014**
- **Kwetsbaarheidsscans en penetratietests van derden**
- **Training van Diligent-medewerkers in gegevensbeveiliging is verplicht**

Functionaliteit

Diligent Messenger is een oplossing die bestaat uit meerdere platforms en die werkt op computers en mobiele apparaten. Diligent Messenger is een tegenhanger van e-mail, waarmee u de productiviteit kunt verhogen en de samenwerking tussen bestuurders kunt verbeteren. Kenmerken:

- **Door de mogelijkheid het scherm van Boards en Messenger gesplitst weer te geven, kunnen bestuurders direct contact opnemen met andere bestuurders terwijl ze bestuursmaterialen bekijken.**
- **Groepsberichten en bijlagen verzenden. Gebruikers kunnen documenten in realtime delen met specifieke bestuurders zodat ze sneller en eenvoudiger kunnen samenwerken.**
- **Gebruikers kunnen in realtime nieuwe voorstellen delen en hierop reageren. Wanneer gebruikers buiten de bestuurskamer discreet en veilig voorstellen kunnen bespreken, zijn ze tijdens de bestuursvergadering minder tijd kwijt.**

Met Diligent Messenger is het mogelijk escalatiemeldingen te verzenden, die per e-mail kunnen worden bezorgd. Een escalatiebericht is een melding aan de gebruiker, die de informatie alleen kan lezen na beveiligde aanmelding bij Diligent Messenger.

Gebruiksvriendelijk

Met Diligent Messenger beschikken bestuurders over een krachtige maar gebruiksvriendelijke oplossing waarmee meer en veiligere samenwerking tussen bestuurders mogelijk wordt gemaakt. Om een overvloed aan e-mail te voorkomen, kunnen bestuurders met Diligent Messenger directer communiceren. Op die manier gaat informatie niet verloren in een overvolle inbox.

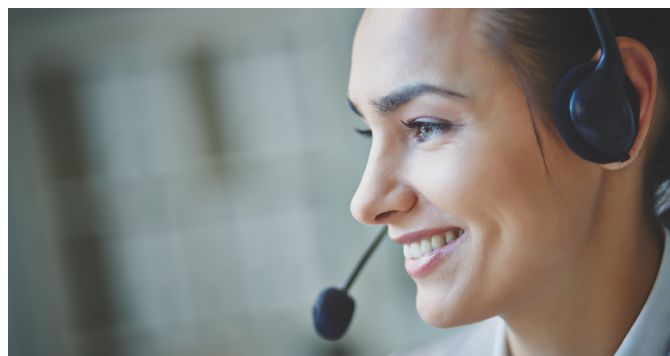
Als een organisatie een oplossing kiest die te complex is, bestaat het risico dat gebruikers de oplossing niet willen gebruiken. Gelukkig biedt Diligent een eenvoudige oplossing met toch een hoog beveiligingsniveau. De initiële installatie van Diligent duurt minder dan twee minuten en de oplossing heeft een vertrouwde en intuïtieve gebruikersinterface. Zoals vermeld, kan Diligent Messenger naadloos worden geïntegreerd met Diligent Boards zodat gebruikers eenvoudig kunnen overstappen en vervolgens kunnen communiceren.

Diligent werkt hard aan het verder ontwikkelen van de technologie en daarbij verbeteren en ontwikkelen we continu nieuwe functies en functionaliteit met Diligent Messenger.

Meer controle en inzicht

Zoals gezegd, heeft het e-mailen van gevoelige bestuursinformatie, met name via privé-e-mail, een negatieve invloed op governance en verantwoording, alsmede op de controle en zichtbaarheid van een organisatie.

Met Diligent Messenger hebben managers, company secretaries en juridische teams nu controle over de bewaartermijn van bestuursberichten, waardoor dit een voorspelbaar en verdedigbaar proces wordt. Met Diligent Messenger bewaart u de informatie die vereist is en verwijdert u de rest volgens uw eigen planning. Met Diligent Messenger kunt u het bewaarbeleid voor documenten van uw organisatie naleven.



Ondersteuning van wereldklasse

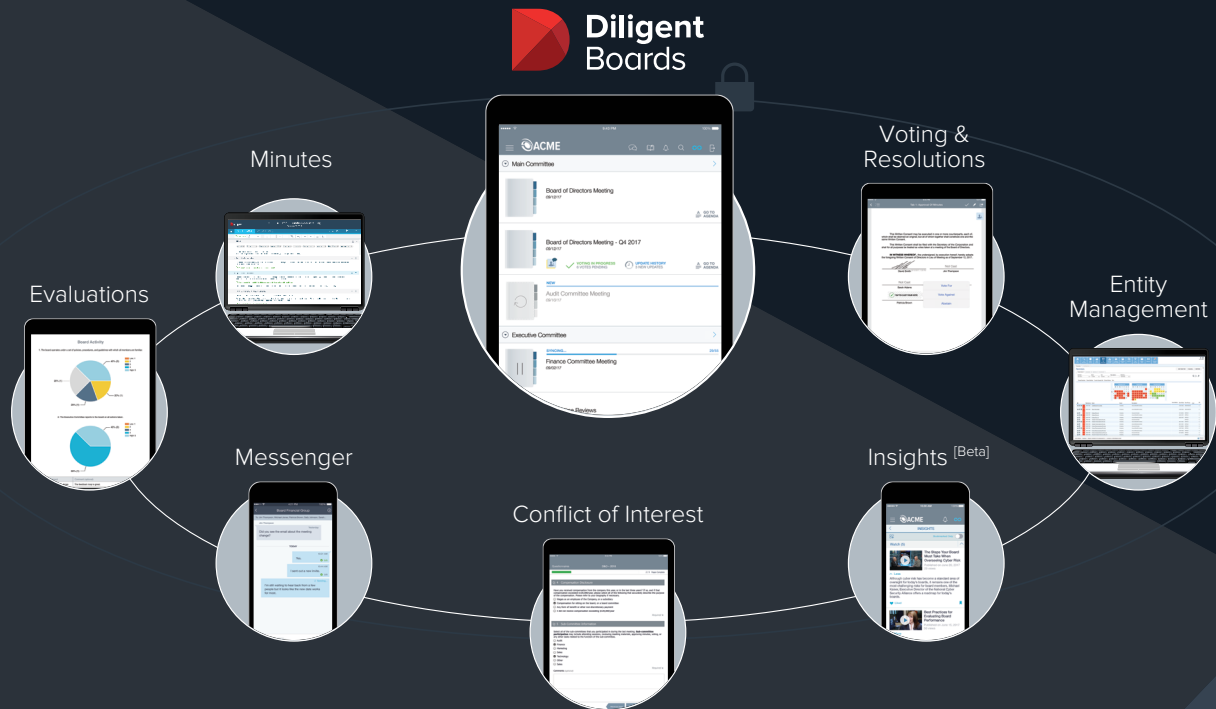
Diligent Messenger wordt ondersteund door het bekroonde Customer Success van Diligent. Integratie en ingebruikname van Diligent Messenger gaat eenvoudig, maar mogelijk hebt u toch vragen of wilt u specifieke training. Diligent kan hierbij helpen. We bieden privétraining en 24/7 support in meer dan zes talen.

CONCLUSIE

Er is geen oplossing die 100% veilig is, maar het is van essentieel belang dat uw bestuurders geen e-mail, sms en andere onveilige communicatiekanalen meer gebruiken. Diligent Messenger levert beveiligde communicatietechnologie rechtstreeks aan bestuurders en beheerders en biedt tegelijkertijd meer inzicht, controle, samenwerking en productiviteit. Diligent Messenger is nauw geïntegreerd met Diligent Boards, waardoor gebruikers beschikken over een vertrouwde interface. Daardoor zullen steeds meer gebruikers de overstap maken zodat de hoge niveaus worden bereikt die nodig zijn om communicatiebeveiliging en -privacy binnen het bestuur te waarborgen. Het geheel aan cyberdreigingen ontwikkelt zich snel. Daarom is het essentieel dat u een oplossingsaanbieder zoals Diligent kiest, die innovatieve beveiligingstechnologie ontwikkelt die vandaag en in de toekomst voldoet aan uw veranderende behoeften.

Nieuw van Diligent:

Governance Cloud™



Start uw reis naar de beste governance met Diligent Boards. Groei met Governance Cloud.

Vereisten op het gebied van governance nemen alsmaar toe.

Eis een partner die met u meegroeit.

Governance Cloud™ is afkomstig van de makers van Diligent Boards en wordt vertrouwd door 65% van de AEX-bedrijven. Met deze oplossing kunnen bestuurders en executives risico's effectiever verlagen en voldoen aan de eisen in de bestuurskamer en daarbuiten.

Diligent heeft meer dan tien jaar ervaring als marktleider en wereldwijd meer dan 12.000 klanten en 400.000 bestuurders en managers als gebruiker. Diligent heeft de afgelopen twee jaar samengewerkt met klanten om de verschillende componenten van Governance Cloud te ontwikkelen. Gebruikers profiteren van de ongeëvenaarde klantenservice van Diligent, gebruiksvriendelijke technologie en vertrouwen in de branche. Governance Cloud kan met u meegroeien.

Start uw reis naar de beste governance.

diligent.com/nl/

