



Bestuursportals: De hoge prijs die u betaalt voor een goedkope oplossing

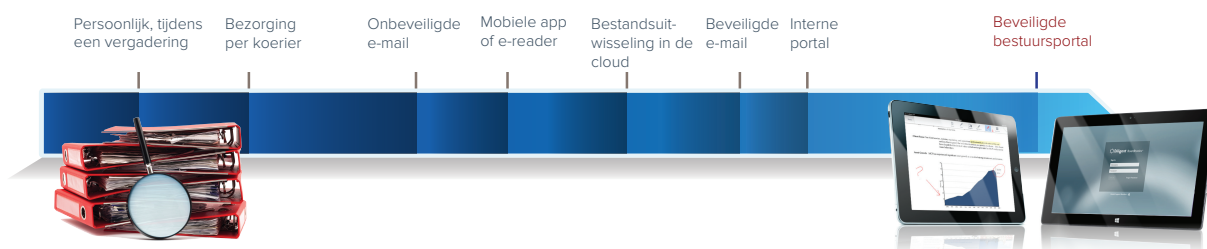
Vandaag de dag zijn er meer redenen dan ooit om over te stappen op digitale bestuurscommunicatie: informatie die niet op tijd beschikbaar is, kwetsbare beveiliging en zorgen over privacy. En die enorme hoeveelheid papier, om nog maar niet te spreken van de wildgroei aan verschillende versies en notities. Maar hoe logisch het ook mag lijken om over te stappen op digitale bestuurscommunicatie, er zijn veel verschillende wegen die een bedrijf kan bewandelen.

OP WEG NAAR DIGITALE BESTUURSCOMMUNICATIE

Organisaties die op weg zijn naar digitale bestuurscommunicatie staan voor een moeilijke keuze. Veel organisaties stappen direct over op portaloplossingen die specifiek gemaakt zijn voor de ondersteuning van besturen, terwijl andere organisaties kiezen voor generieke software of hun eigen interne oplossingen maken, omdat ze denken dat deze alternatieven goedkoper zijn.

Hoewel deze tussenoplossingen wel zorgen voor een bepaalde vorm van digitale bestuurscommunicatie, kunnen ze een gevaar vormen voor de veiligheid, integriteit en actualiteit van essentiële informatie die de prestaties van het bestuur juist moesten verhogen. In plaats van een goedkope verbetering ten opzichte van papier, betalen te veel organisaties juist een hoge prijs voor oplossingen die uiteindelijk de verwachtingen niet waarmaken. En nadat ze met deze problemen te maken hebben gehad, zal de meerderheid afstappen van deze kant-en-klare doe-het-zelfoplossingen en in plaats daarvan beveiligde bestuursportals gaan gebruiken.

Aanlevering van materialen voor bestuursvergaderingen



Diligent

ONBEVEILIGDE E-MAIL

Het gebruik van persoonlijke e-mailadressen mag dan een makkelijke oplossing lijken, maar is doorgaans onveilig en foutgevoelig. Google¹ heeft in het verleden zelfs toegegeven dat het niet waarschijnlijk is dat de inhoud van hun Gmail-service vertrouwelijk is. En bovendien verliest het bedrijf de controle over een e-mail zodra die naar een bestuurslid is verzonden, want het bericht kan altijd worden doorgestuurd. Daarnaast kunnen e-mails ironisch genoeg ook weer leiden tot meer papier. Uiteindelijk drukken bestuursleden e-mailbijlagen vaak af. Zo worden ze niet alleen weer opgezaagd met de ongemakken van papier, wat de reden was waarom ze in de eerste instantie digitaal zijn gaan werken, maar raken ze ook het model van een gebonden vergaderpakket of ordner kwijt, waardoor vergaderingen steeds worden onderbroken.

E-READER-APPS

E-readertoepassingen zoals iAnnotate maken het makkelijker om pdf-bestanden te lezen, te corrigeren en te delen op een iPad. Maar om een beveiliging op bedrijfsniveau te kunnen garanderen, moet iAnnotate voor Good² worden aangeschaft, voor bescherming door de beveiligde containerisatietechnologie van Good. Interessant genoeg wordt hierdoor de toegang van iAnnotate-gebruikers tot onbeveiligde bronnen voor verbinding beperkt, zoals externe cloudopslag en onbeveiligde e-mailtoepassingen. Bovendien zijn pdf-documenten gemaakt met Adobe, dat de gebruikers ervan blootstelt aan kwetsbaarheden in de beveiliging. Onlangs is er broncode van Adobe³ aangetroffen op de eigen server van een hackerscollectief, wat grote gevolgen voor de beveiliging had. Tekortkomingen zoals deze kunnen mogelijk hoge kosten met zich meebrengen als bestuursmaterialen en persoonlijke notities worden gelekt of verkeerd worden opgeslagen.

CLOUDDIENSTEN VOOR HET DELEN VAN BESTANDEN

Met gratis diensten voor het delen van bestanden kunt u gegevens uploaden naar en downloaden uit de cloud. Hoewel deze diensten worden beschermd met behulp van beveiligingsfuncties zoals versleuteling en dubbele authenticatie, zijn ze eerder al gehackt, waardoor bestanden en e-mailadressen van particulieren openbaar zijn geworden. En minder bekende of financieel zwakkere bedrijven voor cloudopslag kunnen van het ene op het andere moment van de aardbodem verdwijnen. Toen Nirvanix, een aanbieder van cloudopslag, aankondigde te gaan stoppen, moesten meer dan duizend klanten op zoek naar een andere opslagoplossing, anders zouden ze hun gegevens voor altijd kwijt zijn.

BEVEILIGDE E-MAIL

Bedrijven kunnen bestuurders een veilig e-mailadres geven. Hierdoor wordt een aantal van de beveiligingsproblemen opgelost die gratis accounts als Gmail met zich meebrengen. Maar bestuurders kunnen nog steeds vertrouwelijke e-mails doorsturen naar onbeveiligde accounts en e-reader-apps gebruiken, en mogelijk terugrijpen op het afdrukken van langere documenten. Ze vinden het misschien ook onhandig om een extra e-mailadres, dat speciaal bestemd is voor bestuurscommunicatie, in de gaten te moeten houden.

INTERNE PORTALS

Organisaties kunnen hun eigen portal bouwen of gebruikmaken van producten zoals Sharepoint, een tool voor samenwerking en documentbeheer. Beide benaderingen hebben zo hun beperkingen. Bestuurders moeten zich waarschijnlijk aanmelden bij het VPN-netwerk van de organisatie voordat ze zich kunnen aanmelden bij de portal, maar zullen dit waarschijnlijk niet gebruiksvriendelijk vinden. Bovendien moet de ondersteuning intern worden afgehandeld. De Company Secretary kan de ondersteuning op zich nemen, maar heeft misschien niet de benodigde vaardigheden of geen toegang tot gespecialiseerde IT-medewerkers om problemen op te lossen en technische vragen te beantwoorden. In beide gevallen kan er geen 24/7 ondersteuning worden geboden. Wanneer u de extra tijd en de overlast waar besturen en interne teams mee te maken hebben, bij elkaar optelt, kunnen de daadwerkelijke kosten van een doe-het-zelfoplossing veel hoger zijn dan die van een externe oplossing met goede ondersteuning.

HET VERSCHIL DAT DILIGENT MAAKT

Diligent Boards™ is de meest gebruikte bestuursportal ter wereld, omdat deze is gemaakt met maar één doel: veilige en intuïtieve toegang tot de informatie die de beste besturen kenmerkt. De portal, die zo intuïtief is dat het gebruik ervan net zo makkelijk is als het lezen van een boek, geeft direct toegang tot bijgewerkte en gearchiveerde vergadermaterialen, en dat in combinatie met de mogelijkheid om notities te delen, om te stemmen en om dezelfde veilige app zowel online als offline te gebruiken. De krachtige beveiliging en privacy zijn overal in het product terug te vinden, van de infrastructuur voor datahosting tot de versleuteling van inhoud zowel tijdens de overdracht als voor de opslag op een apparaat, tot alle beveiligingsprocessen. Iedere klant krijgt toegang tot een gespecialiseerd accountmanagementteam en onbeperkt advies, doorlopende training en het hele jaar door, 24 uur per dag en 7 dagen per week live-ondersteuning per telefoon van Diligent-medewerkers. Diligent helpt besturen al sinds 2001 en heeft een bewezen staat van dienst.

1 Uit 'Google: don't expect privacy when sending to Gmail', *The Guardian*, 14 augustus 2013, <http://www.theguardian.com/technology/2013/aug/14/google-gmail-users-privacy-email-lawsuit>

2 iAnnotate PDF: *Good Dynamics Edition*, 23 oktober 2013, <http://www.branchfire.com/iannotate/>

3 'Adobe gets hacked, product source code and data for 2.9M customers likely accessed', *TechCrunch*, 3 oktober 2013, <http://techcrunch.com/2013/10/03/adobe-gets-hacked-product-source-code-and-data-for-2-9m-customers-likely-accessed/>

4 'Security Researchers Prove That Dropbox Can Be Hacked', *Business Insider*, 28 augustus 2013, <http://www.businessinsider.com/researchers-prove-dropbox-can-be-hacked-2013-8>

5 Uit 'Cloud storage provider Nirvanix is closing its doors', *Infoworld*, 13 september 2013, <http://www.infoworld.com/d/virtualization/cloud-storage-provider-nirvanix-closing-its-doors-227289>



Ons Diligent Boards-product zorgt voor veiligheid, eenvoud en service voor bestuurscommunicatie.

Telefoonnummer:
Nederland: +31 (0) 621 552 222
E-mailadres: info@diligent.com
Ga naar: www.diligent.com/nl/