Cyberdreigingen en het beveiligen van het bestuur: **Drie misvattingen die de beveiliging van de bestuurskamer ondermijnen**

Cyberaanvallen komen wereldwijd steeds vaker voor. Criminelen worden steeds handiger in het omzeilen van beveiligingssystemen en in de media vernemen we steeds vaker over aanvallen die grote impact hebben. Toch wordt de dreiging van cybercrime nog steeds vaak genegeerd. En besturen die wel actie ondernemen, slagen er vaak niet in om zichzelf naar behoren te beschermen. Dit artikel is een reactie op die trend. Wij willen bestuurders en managers inzicht geven in het probleem van cybercrime en tegelijkertijd laten zien hoe zij veiligheidsrisico's op bestuursniveau kunnen verminderen.

De toename van cybercrime heeft verschillende oorzaken. De pakkans is bijvoorbeeld laag vergeleken bij andere soorten misdaad, en gegevens kunnen via duizenden computers worden doorgestuurd, waardoor aanvallen anoniem zijn en niet kunnen worden getraceerd. De meeste cybercrime vindt plaats door georganiseerde misdaad en levert cybercriminelen miljoenen op. Volgens analisten kost dat de mondiale economie jaarlijks USD 455 miljard.[1]

Een geslaagde aanval kan een organisatie gigantische schade toebrengen. Naast financiële verliezen kan diefstal van gegevens en intellectueel eigendom nadelige gevolgen hebben voor handel, concurrentiepositie, innovatie en reputatie. Organisaties kunnen zichzelf beschermen door op een andere manier met gegevens om te gaan en informatie te beveiligen. De kans op een cyberaanval kan zo sterk worden beperkt.

Diligent

1 "Net Losses: Estimating the Global Cost of Cybercrime," McAfee, 2014. http://www.mcafee.com/uk/resources/reports/rp-economic-impact-cybercrime2-summary.pdf

BEVEILIGING VAN HET BESTUUR BEOORDELEN

Leidinggevenden kunnen de cybersecurity van hun bestuur beoordelen door drie eenvoudige vragen te stellen:

Hoe worden de bestuursgegevens opgeslagen?

Elke beveiligingsbeoordeling moet beginnen met een onderzoek naar wie de gegevens controleert. Niet weten waar informatie zich bevindt en niet kunnen controleren waar die informatie heen gaat, betekent dat de oplossing zeer onveilig is.

Daarom is het per e-mail versturen van bestuursstukken als pdf-bestand geen veilige oplossing. Bestanden kunnen per ongeluk door bestuurders worden doorgestuurd naar anderen die geen deel uitmaken van het bestuur, of worden bewaard in persoonlijke e-mailaccounts met minimale beveiliging, op systemen waarvan de leveranciers zelf aangeven dat ze niet als veilig kunnen worden beschouwd.

Hetzelfde geldt voor opslagoplossingen in de cloud, waarbij uw bestanden zich op elke server binnen een netwerk kunnen bevinden, zonder dat u weet waar precies. Het succes van cloudoplossingen is gebaseerd op de veronderstelling dat ze veilig zijn. Maar in werkelijkheid tonen welbekende gevallen van hacken, zoals het bekendmaken van wachtwoorden en foto's van beroemdheden die op cloudserviceproviders[4] stonden, aan hoe onjuist deze veronderstelling is.

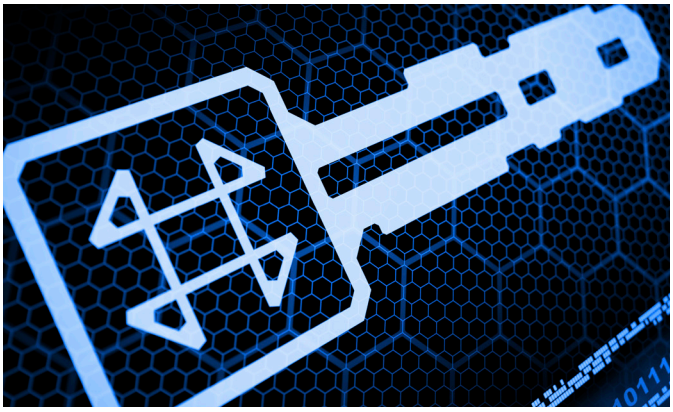
Gehoste bestuursportals lijken op cloudoplossingen en worden vaak ten onrechte zo genoemd, maar er zijn belangrijke verschillen. Gehoste bestuursportals geven nauwkeurige controle over de opslaglocatie van uw gegevens en houden de gegevens van elke gehoste organisatie gescheiden van elkaar. De wetenschap waar de gegevens zich bevinden en hoe ze worden beschermd, zorgt voor meer zekerheid en meer controle over wie toegang tot de informatie heeft.

Hoe stevig zijn de sloten?

Het is niet alleen essentieel om te weten waar uw gegevens zich bevinden, maar ook om ervoor te zorgen dat alleen gemachtigde gebruikers daar toegang toe hebben. Dat kan worden gerealiseerd door de gegevens te versleutelen, waarbij de gegevens worden omgezet in een reeks betekenisloze enen en nullen, waardoor alleen degenen met de juiste digitale sleutel ze kunnen ontcijferen.

Papieren bestuursstukken hebben helemaal geen digitale sleutel: iedereen die een exemplaar in handen heeft, kan de informatie lezen. Pdf's kunnen weliswaar versleuteld worden ge-emaild of opgeslagen op filesharing-systemen, of van een wachtwoord worden voorzien, maar de verzender en de ontvanger van het materiaal zijn degenen die het wachtwoordprotocol moeten beheren. En zelfs dan zijn pdf-documenten kwetsbaar voor zogeheten brute-foce-aanvallen, waarbij algemeen beschikbare software wordt gebruikt.

Bestuursportals waarvan de hosting beter is verzorgd, gebruiken vaak 256-bits versleuteling. Aangezien daar meer combinaties mee mogelijk zijn dan er sterren in het heelal zijn, kunt u gerust stellen dat het bijna een eeuwigheid duurt voordat zelfs de meest vastberaden hackers met behulp van de meest geavanceerde technologie die code kunnen kraken.



Wie beheert de sleutels?

Het maakt niet uit hoe sterk het encryptiesysteem is, iedereen kan met de juiste sleutel toegang tot de informatie krijgen. Iedereen die over het wachtwoord van een beveiligde pdf beschikt, is in feite degene die het document in bezit heeft. Gestolen wachtwoorden staan dus gelijk aan gestolen documenten.

Beveiliging met een wachtwoord is erg beperkt omdat het beheer van de sleutels binnen het systeem ligt. Een sterke portal verliest echter nooit de controle over de documenten. Degene die zich aanmeldt, ziet alleen wat hij of zij mag zien, en als een wachtwoord wordt gestolen, kan de beheerder eenvoudig de toegang met dat wachtwoord onmogelijk maken.

Bij het machtigen van gebruikers kunnen beheerders niet alleen de toegang tot specifieke documenten beperken, maar ook de toegang en zichtbaarheid van documenten voor een gebruikersgroep regelen. Dit is bijvoorbeeld nuttig wanneer een remuneratiecomité informatie niet wil delen met het gehele bestuur.

De beheerder van een gehoste bestuursportal kan bovendien de toegang van apparaten beheren. Een bestuurder kan zo worden uitgesloten van toegang vanaf persoonlijke, minder veilige apparaten, en worden verplicht om bedrijfssystemen te gebruiken. En wanneer gevoelige documenten niet meer nodig zijn, kan de beheerder een 'virtuele schoonmaak' uitvoeren waardoor de documenten per direct worden afgesloten voor diegenen die er toegang toe proberen te krijgen. Op dezelfde manier kan de toegang worden beperkt voor bepaalde gebruikers of apparaten. Dit is handig als een bestuurder uit het bestuur treedt, als materialen moeten worden teruggevonden of als een wachtwoord is gestolen.

GEEF HET VEILIGE VOORBEELD

Cybersecurity, in het bijzonder de veiligheid van informatie en gegevens van het bestuur, moet de hoogste prioriteit hebben. Een veilige, intuïtieve bestuursportal voor alle informatie, communicatie en samenwerkingsmogelijkheden verhoogt de beveiliging van het bestuur en verbetert de werkmethoden.

Wanneer een bestuur er niet in slaagt hoge veiligheidsnormen te hanteren, kan de veiligheid van de organisatie als geheel in gevaar komen. Maar een bestuur dat het goede voorbeeld geeft, verhoogt de effectiviteit van de beveiliging en maakt de organisatie robuust en bestand tegen toenemende dreigingen.

4 BBC News, http://www.bbc.co.uk/news/technology-29011850

UW BESTUUR EVALUEREN

Als beleidsmakers is het essentieel dat bestuurders begrijpen met welke bedreigingen hun organisatie te maken heeft. Dit kan echter lastig zijn. Veel bestuurders beseffen niet hoe digitaal het bedrijfsleven is geworden. Ze hebben geen volledig beeld van de manier waarop IT, enterprisetechnologie en operationstechnologie samen het bedrijfsleven hebben gevormd en hackers meer kansen hebben gegeven om binnen te dringen in bedrijven.

Hiërarchieën binnen de organisatie zijn ook een aandachtspunt. Het feit dat het bestuur 'boven' de organisatie is geplaatst, betekent dat de werknemers die verantwoordelijk zijn voor de veiligheid van de organisatie, misschien wel geen zorgen durven te uiten over het beveiligingsplan van het bedrijf. Onderzoek door Deloitte en Systemec duidt erop dat in sommige regio's maar liefst 70% van de IT-besluitvormers weinig vertrouwen heeft in het beveiligingsbeleid van het eigen bedrijf.[2] De conclusie is dat meer dan twee derde van de organisaties niet in staat is zichzelf te beschermen tegen een aanval. Het komt ook voor dat het beveiligingsteam van een organisatie niet beseft dat het verantwoordelijk is voor de veiligheid van het bestuur en ervan uitgaat dat dit een taak is van de bedrijfssecretaris.

Een bestuur moet weten welke bedreigingen er voor de eigen organisatie bestaan. Maar dit kan lastig zijn: veel bestuurders beseffen niet hoe digitaal het bedrijfsleven is geworden.

Een andere factor is dat de acties die bestuurders zelf ondernemen, direct bijdragen aan de verhoogde veiligheidsrisico's die het bestuur loopt. Door bestuursstukken op een gemakkelijke, maar onveilige manier te openen, op te slaan en te verspreiden, stellen bestuurders deze gegevens bloot aan derden en hebben ze er geen controle meer over. E-mail, pdf en cloudopslagsystemen bijvoorbeeld zijn vaak veel minder veilig dan de methoden die door de organisatie worden toegepast.

Bestuurders en personeel moeten zorgvuldig blijven omgaan met communicatietechnologie. Maar ook de veiligste methoden kunnen worden ondermijnd door misvattingen die heersen over de gebruikte technologie en workflows.

DE DRIE MISVATTINGEN OMTRENT BEVEILIGING

Neem de volgende misvattingen in acht om te voorkomen dat bestuurders op zo'n manier te werk gaan dat de veiligheid van het bestuur wordt ondermijnd.

1. E-mail is veilig

E-mail is een handige, snelle en gemakkelijke manier om vertrouwelijke informatie over te brengen. Maar eigenlijk is e-mail daarvoor niet geschikt: u kunt het doorsturen van inhoud immers niet beperken. Bovendien is het lastig om een verzonden bericht terug te halen. Zodra een e-mail is verzonden, bent u in feite de controle over de informatie kwijt.

2. Bescherming met wachtwoorden is beveiliging

Het lijkt redelijk om aan te nemen dat een pdf met een wachtwoord ontoegankelijk is voor niet-gemachtigde gebruikers. Maar een eenvoudige zoekopdracht op een populaire zoekmachine geeft miljoenen resultaten voor het omzeilen van pdf-beveiliging. Probeer het maar eens op Google. U zult meer dan 2.300.000 resultaten vinden waaruit blijkt hoe eenvoudig het is om dit ogenschijnlijk veilige medium te kraken. In werkelijkheid is pdf-technologie niet veilig, en mag u er niet op vertrouwen.

3. Interne opslag van gegevens is veiliger

De belangrijkste misvatting is dat interne opslag van gegevens veiliger is dan opslag bij een derde partij. In werkelijkheid is vaak het omgekeerde het geval. Interne oplossingen zijn ervan afhankelijk dat de beheerders van de organisatie zelf gegevens beheren, maar aangezien 55% van de cyberaanvallen wordt uitgevoerd door insiders, kan deze benadering catastrofaal zijn.[3] Daarnaast bieden het eigen veiligheidsplan en de eigen infrastructuur van de organisatie vaak onvoldoende bescherming tegen de bedreigingen van vandaag de dag. Een SaaS-leverancier als Diligent daarentegen beperkt de toegang tot gegevens uitsluitend tot gemachtigde gebruikers van de klant: ons team heeft absoluut geen toegang tot gegevens van klanten. Bovendien hanteren wij op alle mogelijke manieren gecontroleerde beleidsregels en procedures voor beveiliging. Wij leveren niet alleen functies voor back-up en herstel van gegevens, maar gaan ook veel verder in het monitoren van de beveiliging dan de meeste andere bedrijven.

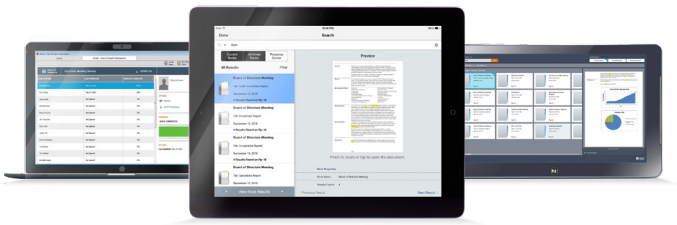
2 Global Risk Insights, september 2015. "globalriskinsights.com/2015/09/how-strong-are-the-middle-easts-cybersecurity-networks/
3 "IBM 2015 Cyber Security Index" en "IBM X-Force Threat Intelligence Quarterly Q2 – 2015" https://securityintelligence.com/the-threat-is-coming-from-inside-the-network/

Diligent

De waarde van informatie volledig benutten. Veilig.

Diligent helpt 's werelds meest toonaangevende organisaties om de kracht van informatie en samenwerking veilig en optimaal te benutten door besturen en managementteams in staat te stellen betere beslissingen te nemen. Meer dan 4000 klanten in meer dan 70 landen vertrouwen op Diligent voor onmiddellijke toegang tot hun meest tijdgevoelige en vertrouwelijke informatie, maar ook op de tools waarmee ze deze informatie kunnen doornemen, bespreken, en er met de belangrijkste beleidsmakers aan kunnen samenwerken. Diligent Boards versnelt en vereenvoudigt de manier waarop bestuursmaterialen worden gemaakt en via iPad, Windows-apparaten en browsers worden verspreid. Tegelijkertijd biedt Diligent Boards praktische voordelen zoals verlaging van de productiekosten, ondersteuning van duurzaamheidsdoelstellingen en besparing van administratie- en IT-tijd.

Join the Leaders. Get Diligent



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

Telefoon: +31 621 552 222
E-mail: info@diligent.com
Ga naar: www.diligent.com

AICPA SOC | ISO 27001 GECERTIFICEERD DOOR BRIGHTLINE | Download in de App Store | Get it from Microsoft