Ga mobiel met uw onderneming: De Executive Checklist

Mobiele mogelijkheden

Hoewel de overgang van mobiele telefoons naar computers er al heel lang aan zit te komen, is de grote overvloed aan veranderingen de afgelopen twee jaar indrukwekkend geweest: Mobiele apparaten zijn erg gewild bij consumenten en bieden zakelijke gebruikers een krachtig medium om mee te leren, handelen, delen en te laten zien dat bedrijven graag investeren in de toekomst.

Een mobiele onderneming betekent nieuwe kansen voor uw organisatie. Werknemers zijn gelukkiger en productiever wanneer zij mobiele toegang hebben tot hun e-mail, apps en gegevens op tablets en smartphones. Bedrijven die werken met oplossingen voor mobiele werkstijl hebben hiermee een voordeel op de concurrentie en sturen aan op groei.

Uit een recent onderzoek, uitgevoerd door Aberdeen, is gebleken dat de beste ondernemingen binnen hun specifieke gebieden veel vaker dan alle andere ondernemingen hun workflow verbinden met mobiele apparaten.[1] Wat volgens bijna elk onderzoek de mobiliteit voor grote ondernemingen en "bring your own device" (BYOD)-programma's tegenhoudt is beveiliging. CSO Magazine heeft recentelijk vermeld dat 17 procent van ondernemingen al wel eens te maken heeft gehad met een lek binnen de mobiele beveiliging.[2]

En toch...

Dit is waar het op neerkomt. Het auditcomité, C-Suite en ook besturen zijn het erover eens - zelfs terwijl ze zelf heerlijk tikken op hun favoriete apparaten - dat het een riskant voorstel is om werknemers hun eigen apparaten te laten kiezen en dan toegang te geven tot zakelijke bronnen, apps en gegevens. In tegenstelling tot normale, beveiligde pc's of goed beheerde BlackBerry®-apparaten, lopen de mobiele apparaten binnen de ondernemingen van vandaag veel uiteen, zijn ze op verschillende manieren kwetsbaar en bieden ze geen standaard manier voor IT om zelfs de meest basale manier van beveiliging te beheren zoals een wachtwoord.

Met een groeiend aantal bedrijven dat gevoelige zakelijke documenten deelt met hun raad van bestuur via de Apple® iPad®, zijn de consequenties van een gegevenslek gemakkelijker voor te stellen. Met nog steeds de gegevenslekken in het achterhoofd die in het midden van de jaren 2000 veel bedrijven ten onder hebben laten gaan en nu ze zelf ook verantwoordelijk gehouden kunnen worden dankzij Sarbanes-Oxley, is het voor executives en bestuursleden noodzakelijk dat hun organisaties mobiele apparaten goed en veilig beheren.

Mobiele veiligheidsproblemen

Hoewel mobiele veiligheidsproblemen variëren van het instellen van wachtwoorden tot het versleutelen van apparaten, staat gegevenslekken bovenaan de lijst van ondernemingen die programma's op het gebied van mobiele werkstijl willen invoeren. Volgens de beveiligingsexpert voor ondernemingen, Jack Gold, zullen organisaties elk jaar drie tot vier keer zoveel smartphones kwijtraken als notebooks. Gold vroeg ons (retorisch) "hoeveel dossiers zal een verloren smartphone of tablet bevatten met 32 of 64 GB aan geheugen?"[3] Met een geschatte waarde van meer dan $ 250 per verloren dossier,[4] kan een gegevenslek een duur grapje worden. Sommige onderzoeksresultaten tonen aan dat de gemiddelde kosten van een mobiele lek neerkomt op meer dan $ 400.000 voor een onderneming en meer dan $ 100.000 voor MKB,[5] en in sommige gevallen kunnen deze kosten variëren in de miljoenen.[6] Deze zorgen blijven groeien omdat een steeds groter aantal smartphones en tablets niet alleen verbinding maakt met het zakelijke netwerk, maar ook toegang heeft tot een steeds groter wordend aantal zakelijke apps en content repositories. Behalve over de gegevens, maken de afdelingen IT en beveiliging van ondernemingen zich zorgen over de risico's van het openstellen van het interne netwerk voor een uitgebreide reeks aan mobiele apparaten. In veel gevallen worden mobiele apparaten niet beheerd of gecontroleerd, dit betekent dat zij bedreigingen kunnen introduceren op het netwerk en een negatieve invloed kunnen hebben om de compliancestatus van een organisatie.

Er zijn drie belangrijke factoren die bijdragen aan de veiligheidsgerelateerde zorgen van ondernemingen

1. Met het rapport van het Center for Telecom Environment Management Standards dat 78 procent van de organisaties het toestaat dat werknemers hun eigen mobiele apparaten meenemen binnen de zakelijke omgeving[7], en de uitgaven van IT-afdelingen binnen ondernemingen van bijna $ 16 miljard in 2013 aan Apple® iPad®-tablets,[8] schiet het volume van mobiele apparaten binnen ondernemingen niet omhoog, maar worden ze daarnaast niet langer uitsluitend gebruikt door executives, maar ook door de normale werknemer. Daarnaast groeit het aantal apps op die apparaten ook nog steeds, onafhankelijk van het feit of het nu een zakelijk mobiel apparaat is of een mobiel apparaat van de werknemer zelf. Asymco, een mobiel analysebedrijf, meldde een gemiddelde van 60 apps per iOS®-apparaat.[9] En omdat meer dan de helft van de organisaties meer dan een apparaatsoort ondersteunt,[10] is de blootstelling van het zakelijk netwerk aan mogelijke non-compliant of schadelijke apps uitermate groot.

2. Mensen op alle niveaus van de organisatie hebben een sterke wens om de medewerkers te voorzien van mobiele apparaten en mobiele toegang tot zakelijk apps en gegevens. Organisaties gaan ook mobiel in de breedte, verspreid over hun hele branche. Hierbij moet u denken aan restaurantketens die hun hosts en keukenpersoneel voorzien van een iPad tot luchtvaartmaatschappijen die de "flight bag" voorzien van elektronische vliegtuighandleidingen, vluchtplannen en compliancedocumenten aan hun luchtvaartpersoneel op hun Samsung Galaxy Tabs. Deze vorm van mobiele toegang belooft veel, maar het betekent ook dat zakelijke gegevens en netwerktoegang in handen zullen zijn van een groter aantal gebruikers via een groeiend aantal apparaten, waardoor de risico's dus worden vermenigvuldigd.

3. Hoewel de meest gehoorde beveiligingsoplossing voor mobiliteit voor grote ondernemingen zich veelal richt op het vergrendelen of wissen van een verloren of gestolen apparaat, is de grootste bedreiging het onbeheerd delen van gegevens. Met miljoenen gebruikers die gegevens delen over een eindeloos aantal via de cloud verbonden eindpunten, valt de kans op een datalek in het niet vergeleken met het scenario waarbij een apparaat wordt verloren/gestolen. Volgen het Citrix Mobile Device Management Cloud Report worden sommige van de meest gebruikte apps, zoals Dropbox en Evernote, ook het meest op de blacklist geplaatst door bedrijven, wat aangeeft dat ze tegelijk heel handig zijn en een risico vormen.[11]

Dit zijn enkel een paar activiteiten die gevaarlijk kunnen zijn voor gevoelige gegevens en de onderneming blootstellen aan mobiele bedreigingen. Het is nu tijd voor een veilige beheeroplossing voor mobiele apparaten, die realtime verdediging biedt binnen alle lagen van de mobiele onderneming.

Met Citrix kan het auditcomité gerust ademhalen

Citrix XenMobile™ biedt de real-time verdediging die een onderneming nodig heeft om de zakelijke mogelijkheden te grijpen die mobiel zakendoen met zich meebrengt, terwijl het de zakelijke IP, klant- en werknemergegevens, niet-openbare financiële informatie en bedrijfsinformatie beveiligt. Met het cloudgebaseerde en on-premise aanbod van Citrix, kunnen uw IT-professionals de meest uiteenlopende reeksen mobiele apparaten beveiligen en beheren, kunnen ze inzicht krijgen in mobiele apps en deze beheren, en kunnen ze het zakelijke netwerk beveiligen tegen mobiele bedreigingen.

XenMobile biedt uw organisatie:

- **MDM voor de onderneming.** Laat gebruikers kiezen welk apparaat ze gebruiken, zonder dat dit van invloed is op uw compliancevereisten.
- **Beveilig e-mail, browser en apps om gegevens te delen.** Productiviteitsapps waar gebruikers van zullen houden en die door IT zullen worden omarmd.
- **Mobiele app-containers.** Gebruikers krijgen de apps die ze nodig hebben en IT voldoet aan de compliancevereisten.
- **Een geünificeerde app store.** Help uw bedrijf door overal toegang tot apps mogelijk te maken.
- **Geavanceerde administratie en eenvoudige gebruikerstoegang.** Beheer gebruikerstoegang en maak de gebruikerservaring een stuk gemakkelijker.

Uw rol binnen de mobiele strategie van uw onderneming

U kent de risico's en u bent bekend met Citrix en XenMobile, onze veilige oplossing op het gebied van beheer van mobiliteit voor grote ondernemingen. U bent er nu helemaal klaar voor om de organisatie binnen uw IT-afdeling te helpen en om de rest van uw bedrijf mobiliteit voor grote ondernemingen aan te laten nemen en gebruik te laten maken van de vele zakelijke mogelijkheden die het met zich meebrengt. Ga nu verder en leid uw bedrijf de toekomst in.

Executive Checklist

☑ Apparaatoverwegingen	• **Bedrijfsdoelen:** Definieer uw bedrijfsdoelen voor mobiliteit voor grote ondernemingen. Specificeer of u zich richt op productiviteitsverbeteringen, de beste mogelijkheden en/of de vrijheid van werknemers wat betreft apparaten. Zorg ervoor dat de mobiele strategie van uw bedrijf deze doelen vertegenwoordigt. • **Apparaatvrijheid t.o.v. apparaatsamenhang:** Zorg ervoor dat uw IT-professionals afwegingen hebben gemaakt met betrekking tot apparaatvrijheid en keuze of samenhang en controle. Zorg ervoor dat zij (en u) vertrouwd zijn met de verschillende soorten apparaten en het beheer en de beveiliging die de apparaten IT bieden. • **BYOD t.o.v. zakelijk eigendom:** Als u niet kunt kiezen tussen 100% zakelijk eigendom en "bring-your-own-device"-programma, kijk dan of een combinatie van de twee misschien meer geschikt is voor uw bedrijf. U kunt bijvoorbeeld bepaalde gebruikers hun apparaatsoort laten kiezen (misschien van een korte lijst) terwijl u de keuze voor andere gebruikers beperkt tot maar één apparaat. Een ziekenhuis kan bijvoorbeeld een BYOD-programma uitrollen voor zijn permanente doktoren en administratieve medewerkers, terwijl het daarnaast zakelijke tablets biedt die op de campus moeten blijven voor de verpleegkundigen.
☑ Gebruikersoverwegingen	• **Mobiele enablement en toelating:** Bepaal wie er mobiel moet zijn (Executives? Sales? Werknemers? Iedereen?). Als het antwoord hierop is dat niet iedereen mobiel hoeft te zijn, bepaal dan welke afdelingen, functies (d.w.z. managers en hoger) en/of bedrijfsredenen in aanmerking komen om mobiel te zijn. Bepaal ook of dit verschillend is voor gebruikers in het veld of wanneer ze geen fulltime werknemers zijn. • **Wie betaalt voor BYOD?:** Bepaal of uw organisatie een BYOD-programma zal invoeren en bepaal wat uw instelling zal zijn met betrekking tot het tolereren, aanmoedigen of zelfs het volledig of gedeeltelijk subsidiëren van de mobiele en/of draadloze kosten. • **Aantal apparaten per gebruiker:** Bepaal of een aantal gebruikers meerdere apparaten kunnen gaan gebruiken met een oplossing op het gebied van mobiliteit voor grote ondernemingen. Kunnen salesmedewerkers bijvoorbeeld hun tablets gebruiken voor demonstraties naast het gebruik van hun telefoon?
☑ App-overwegingen	• **Welke apps laat u toe?** Zorg ervoor dat uw IT-afdeling goed heeft nagedacht over welke mobiele apps ondersteund zullen worden door uw organisatie (alleen e-mail, contactpersonen, agenda? Bedrijfsautomatisering? ERP? Aangepaste apps?). Zorg ervoor dat hun plan voor het uitrollen van apps duidelijk past bij de behoeften en het risicoprofiel van uw bedrijf. Zorg ervoor dat de toegang tot apps die mogelijk wordt gemaakt door IT kan verschillen per functie, groep, apparaat, en of het apparaat zakelijk of persoonlijk eigendom is. • **Hoe gaat u apps beveiligen?:** Zorg ervoor dat IT de mogelijkheden heeft om de mobiele apps en bronnen te beperken, ongeacht het soort gebruiker of apparaat dat u kiest. Ze moeten de mogelijkheid hebben om zelf-ontwikkelde apps, apps van derden of BYO mobiele apps te beveiligen met uitgebreide, beleidsgebaseerde controlemaatregelen, inclusief mobiele DLP en andere benodigdheden zoals het op afstand kunnen locken, wipen en versleutelen van apps en gegevens. • **Mobiele zakelijke mogelijkheden:** Ken de mobiele doelen en tijdlijnen van uw zakelijke branche. Zorg ervoor dat IT rekening houdt met de intenties van uw LOBs om hun favoriete apps mobiel te maken voor hun gebruikers en partners, en of zij de intenties hebben om aangepaste apps te ontwikkelen of uit te breiden voor bepaalde apparaten.

☑ Gegevensoverwegingen	• **Wat zijn de regels omtrent gegevens?** Bekijk het IT-beleid van uw organisatie met betrekking tot de mobiele toegang tot gegevens en zorg ervoor dat uw organisatie beleidslijnen kan opzetten per functie, groep, apparaat en zelfs context voor wie er toegang zal krijgen tot apps en data repositories die intellectuele eigendommen, persoonlijke informatie, bedrijfsinformatie, niet-openbare financiële gegevens, toekomstige aankondigingen, etc. bevatten. Daarnaast zullen veel gebruikers meer dan één apparaat hebben en moet u er dus voor zorgen dat gebruikers op dezelfde veilige manier toegang moeten kunnen krijgen tot gegevens in hun apps, het web en datacenters over meerdere apparaten. • **Risico van gegevenstoegang:** Bepaal de waarde en het risico van de gegevens waar werknemers toegang tot zullen krijgen en bepaal de consequenties van gegevensverlies of een lek. Zorg ervoor dat u en uw executive team/raad zich op het gemak voelen met de winst-verlies-afweging. • **Voorkomen van gegevenslek:** Zorg ervoor dat uw IT-organisatie gevoelige gegevens kan beschermen. Zorg ervoor dat uw IT-organisatie plannen heeft voor hoe het het lekken van gevoelige gegevens via mobiele apparaten zal voorkomen. • **Samenwerking faciliteren:** Zorg ervoor dat u naast het beschermen van gegevens er ook voor zorgt dat personen die toegang nodig hebben tot deze gegevens dit ook kunnen krijgen en hier gemakkelijk mee om kunnen gaan. Het stroomlijnen van de toegang zal uw beveiligingsmaatregelen ondersteunen omdat gebruikers minder snel om deze maatregelen heen zullen proberen te werken.
☑ Beleidsoverwegingen	• **Compliancenormen:** Bekijk de regelgevende-, sector- en zakelijke beleidsregels waaraan uw organisatie zich moet houden (regelgevingen zoals HIPAA, industriële richtlijnen zoals PCI, richtlijnen zoals die van het SEC, IT-kaders zoals ITIL, andere zakelijke beleidsregels) en zorg ervoor dat uw mobiele strategie uw huidige compliancemaatregelen ondersteunt. • **Privacy en globale overwegingen:** Bekijk de buitenlandse wetgevingen en regelgevingen voor regio's waarin uw bedrijf werkzaam is of klanten bedient en zorg ervoor dat uw mobiele strategie uw naleving van deze beleidsregels ondersteunt. Hieronder valt niet alleen de beveiliging, maar ook het privacybeleid van gebruiker die mogelijk aangeven hoe u uw oplossing op het gebied van mobiliteit voor grote ondernemingen moet implementeren op verschillende locaties waarop u werkzaam bent. Bekijk uw beleidsregels voor mobiele apparaten en toegang (beleidsregelinstellingen, overzicht en rapportage) met uw auditcomité, C-Suite en de raad van bestuur. • **Mobiel contract van de werknemer:** Zet beleidsregels op met duidelijke overwegingen en beperkingen omtrent de eigendom, aansprakelijkheid, vervanging, ondersteuning en controle van het apparaat. Naast de beveiliging en toegangsregels dient u ook rekening te houden met het mobiele "contract" tussen het bedrijf en de gebruikers. Wie is de eigenaar van het apparaat en wie betaalt er voor de diensten? Wie is er verantwoordelijk voor de vervanging van het apparaat? Naast dit alles dient u duidelijke beleidsregels op te stellen rondom de uittreding van een apparaat bij vertrek van een werknemer. • **Minimale beleidsvereisten:** Bepaal de mate van uw flexibiliteit voor de apparaten die niet mee zullen doen in een volledige oplossing voor mobiliteit voor grote ondernemingen. Past u de beleidsregels bijvoorbeeld zo aan dat bepaalde gebruikers zoals aannemers en gebruikers in bepaalde regio's nog steeds toegang hebben tot hun e-mail en/of andere belangrijke apps op hun mobiele apparaten zonder inbreuk te maken op de privacy van de gebruiker? • **Vergoedingen:** Als u een BYOD-programma invoert, biedt u dan een vergoeding voor het apparaat en/of de dienst? Als dit het geval is, hoe beheert u dit dan en wie zal hier dan voor in aanmerking komen? Zult u nog steeds gebruik kunnen maken van volumekortingen van serviceproviders?

☑ Beveiligingsoverwegingen	• **Apparaat, gebruiker en app-compliance:** Begrijp hoe uw IT-organisatie om zal gaan met de aanwezigheid van malafide apparaten, onbevoegde gebruikers en non-compliant mobiele apps op het netwerk. • **Gegevensbeveiliging:** Begrijp hoe uw IT-organisatie zakelijke gegevens zal beveiligen tegen onbevoegde toegang, per ongeluk verlies en bedreigingen van binnenin. • **Controleren van bedreigingen:** Begrijp hoe uw IT-organisatie uw beveiligingsinfrastructuur zal controleren op beveiligingsrisico's en de prestaties van het netwerk, de app en het apparaat. Als u een logboekbeleid hebt voor compliance- en gerechtelijke doeleinden, zorg er dan voor dat zij zijn uitgerust om die logboeken te verzamelen, te behouden en te beschermen. • **Buitengebruikstelling:** Begrijp hoe uw IT-organisatie gegevens zal verwijderen van apparaten wanneer deze zijn verloren of gestolen of wanneer een werknemer vertrekt. Als u van plan bent persoonlijke apparaten toe te laten binnen de werkplek, bekijk dan uw plan om zakelijke gegevens te verwijderen terwijl u de persoonlijke inhoud intact laat. Zorg ervoor dat u een plan heeft om duidelijk de beleidsregels en processen bekend te maken bij de betreffende werknemers. • **SIEM-integratie:** Begrijp of uw IT-organisatie uw beheersysteem voor mobiele apparaten zal integreren met een beveiligingssysteem o.i.d. dat informatie en events beheert, en zorg ervoor dat er een plan is om dit te doen.
☑ Schaalbaarheid en overwegingen bij hoge beschikbaarheid	• **Uptime:** Zorg ervoor dat uw IT-organisatie een uptime service-level overeenkomst heeft opgesteld en kan ondersteunen, en of het uw bedrijfsbenodigdheden uitlijnt. • **Bedrijfsgroei:** Zorg ervoor dat uw mobiele strategie rekening houdt met groei en ervoor zorgt dat uw IT-organisatie alle gebruikers kan ondersteunen die u vandaag maar ook later wilt mobiliseren. • **Kosten van de schaalbaarheid:** Zorg ervoor dat uw mobiele strategie het voor u mogelijk maakt om gebruikers op een rendabele manier te schalen en dat alle bijkomende hardware-, software- en servicekosten begroot worden. • **Redundantie en fouttolerantie:** Begrijp het hoge beschikbaarheidsplan van uw mobiele strategie. Als uw strategie load balancing, server en gegevensredundantie en (als het gaat om een cloudgebaseerde oplossing) globale redundantie voor rampenherstel bevat, zorg er dan voor dat deze investeringen terugkomen in het plan.
☑ Service-overwegingen	• **QoS-overwegingen:** Begrijp of uw mobiele strategie het controleren van de servicekwaliteit van telecommunicatie bevat. Als dit het geval is, zorg er dan voor dat uw IT-organisatie duidelijk kan maken welke acties u zult ondernemen met betrekking tot de bedrijfsinformatie die u vergaart. • **Telecomkosten:** Begrijp of uw mobiele strategie het beheren van de kosten van telecommunicatie omvat. Zorg ervoor dat u uw besparingsdoelen en meetmechanismes duidelijk hebt gemaakt voor het evalueren van uw voortgang ten opzichte van die doelen. • **Ondersteuning op afstand:** Begrijp of uw mobiele strategie het leveren van ondersteuning, diagnose en probleemoplossing op afstand impliceert, en welke mechanismes op hun plaats zijn om dit te doen. • **Self-service van de werknemer:** Begrijp of uw IT-organisatie van plan is een self-service portal aan te bieden voor gebruikers om de basic beveiligings- en beheeracties op hun apparaten mee uit te kunnen voeren.

Over Citrix XenMobile

Citrix XenMobile is een mobiliteitsbeheeroplossing voor grote ondernemingen die de volledige vrijheid biedt voor mobiele apparaten, apps en gegevens. Werknemers krijgen via één enkele klik snel toegang tot al hun mobiele, web-, datacenter- en Windows-apps vanuit een verenigde applicatieopslag, inclusief prachtige productiviteitsapps die naadloos zijn geïntegreerd om een geweldige gebruikerservaring te bieden. De oplossing biedt op identiteit gebaseerde provisioning en beheer voor alle apps, gegevens en apparaten, op beleid gebaseerd beheer zoals beperking van de toegang tot de app voor geautoriseerde gebruikers, automatische de-provisioning van de account voor afgesloten gebruikers en selectieve wipe van apps en gegevens die zijn opgeslagen op verloren, gestolen of out-of-compliance apparaten. Met XenMobile kan IT voldoen aan de wensen van de gebruikers om apparaten zelf te kunnen kiezen terwijl het datalekken kan voorkomen en het interne netwerk kan beveiligen tegen mobiele bedreigingen.

1. “Mobility in ERP 2011”, Kevin Prouty, Aberdeen, mei 2011
2. “Global State of Information Security Survey”, CSO Magazine, 2012
3. “MDM is No Longer Enough”, Citrix-webinar met de ondernemingsbeveiligingsexpert, Jack Gold, oktober 2011
4. “U.S. Cost of a Data Breach”, Ponemon Institute, maart 2011
5. State of Mobility Survey, Symantec, februari 2012
6. In 2010 waren de gemiddelde kosten van een gegevenslek $ 7,2 miljoen. Doug Drinkwater, Feb. 10, 2012, TABTIMES.COM
7. marketwatch.com/story/ctemsr-research-78-of-enterprises-allow-bring-your-own-device-byod-2012-07-24?siteid=nbkh
8. “Global Tech Market Outlook for 2012 and 2013” Andrew Bartels, Forrester, 6 januari 2012
9. “More Than 60 Apps Have Been Downloaded for Every iOS Device”, Asymco, 16 januari 2011
10. “Market Overview: On-Premises Mobile Device Management Solutions”, Forrester, 3 januari 2012
11. Citrix Mobile Device Management Cloud Report, Q3 2012

CITRIX®

Over Citrix

Citrix (NASDAQ:CTXS) is het cloudbedrijf waarmee mobiele werkstijlen mogelijk gemaakt worden - waardoor mensen overal kunnen werken op een eenvoudige en veilige manier. Met marktleidende oplossingen voor mobiliteit, desktopvirtualisatie, cloudnetwerken, cloudplatforms, samenwerking en gegevensuitwisseling, helpt Citrix organisaties de benodigde snelheid en flexibiliteit te realiseren die nodig zijn om te slagen in een mobiele en dynamische wereld. Citrix-producten worden gebruikt bij meer dan 260.000 organisaties en door meer dan 100 miljoen gebruikers wereldwijd. De jaaromzet in 2012 was $ 2,59 miljard. Meer informatie op www.citrix.nl.

0513/PDF **citrix.nl**