
BEST PRACTICES
MOBILE DEVICE MANAGEMENT
EN MOBILE SECURITY.
With Kaspersky, now you can.
kaspersky.nl/business
Be Ready for What's Next
KASPERSKY lab

INHOUD

MOBILE DEVICES: HET NIEUWSTE DOELWIT VAN CYBERCRIMINELEN

1. 24/7 MOBIELE TOEGANG

Medewerkers verwachten 24/7 mobiele toegang tot bedrijfsapplicaties en informatie. Het stelt hen in staat productiever en meer flexibel te zijn.

Dit heeft echter een keerzijde: de functies die apparaten zo aantrekkelijk maken voor werknemers maken ze ook zeer aantrekkelijk voor hackers, gegevensdieven, verspreiders van malware en andere criminelen. Alleen al in de afgelopen twaalf maanden heeft 51% van alle organisaties wereldwijd te maken gehad met gegevensverlies vanwege slecht beveiligde mobiele apparatuur.[1]

Dit wordt niet uitsluitend veroorzaakt door malware; de trend 'Bring Your Own Device' (BYOD) in bedrijven van elke omvang zorgt ervoor dat bedrijven een steeds complexere reeks apparaten moeten beheren. Ondertussen vervagen de grenzen tussen zakelijk en persoonlijk gebruik, waardoor beheerders steeds meer worden belast met het beheer van de IT-omgeving.

Hoe kunt u zonder kopzorgen ondersteuning bieden voor BYOD-initiatieven? Hoe kunt u het gedrag van eindgebruikers in de gaten houden als ze apps downloaden in een hotelkamer of een andere tijdzone? Wat gebeurt er als zij hun smartphone in de taxi laten liggen? Kunt u dit alles eenvoudig vanuit één centraal punt beheren? Mobile Device Management (MDM) biedt het antwoord op deze vragen.

2. MOBILE DEVICE MANAGEMENT – WAT IS DAT?

Met Mobile Device Management kunnen IT-professionals hun 'bekabelde' beveiligingsstrategie en het beheer toepassen op alle apparaten, waar die zich ook bevinden. Via MDM-software kunnen IT-beheerders vitale beheer- en bewakingstaken, zoals apparaatconfiguratie, software-updates en back-up/herstel, rendabel automatiseren. Gevoelige bedrijfsinformatie is beschermd in geval van diefstal, verlies of misbruik door de eindgebruiker.

3. DE JUISTE MDM-OPLOSSING KIEZEN

3.1 Ondersteuning voor meerdere platformen

Android, BlackBerry, iOS, Symbian, Windows Phone. Als uw organisatie BYOD-initiatieven ondersteunt, weet u hoe lastig het is om meerdere platformen te beveiligen en te onderhouden.

Een MDM-oplossing met ondersteuning voor meerdere platformen is niet alleen rendabel, maar maakt het beheer van meerdere systemen ook een stuk eenvoudiger. MDM levert ook flexibiliteit op, waardoor niet alleen uw huidige apparaten, maar ook de merken en producten die u in de toekomst kiest worden ondersteund.

1 Bron: Ponemon: The Cost of a Lost Laptop (2009)

4. MOBILE DEVICE MANAGEMENT – BEST PRACTICES

4.1 Duidelijke beleidsregels

Maak specifieke beleidsregels voor mobiele apparatuur waarin onder meer de onderstaande items duidelijk worden gedefinieerd:

- Hoe het apparaat wordt gebruikt
- Welke gegevens beschikbaar zijn voor mobiele gebruikers
- Wie wat mag doen op het bedrijfsnetwerk
- Welke procedures worden gehanteerd in geval van verlies of diefstal

U moet beleidsregels op een flexibele, gedetailleerde manier definiëren en afdwingen – bijvoorbeeld door verschillende regels voor verschillende gebruikers en groepen te definiëren. Dit detailniveau moet zijn gericht op het apparaat zelf, bijvoorbeeld door te voorkomen dat gekraakte of anderszins geïnfecteerde apparaten toegang hebben tot bedrijfsgegevens of door deze op afstand te vergrendelen. Dit vormt een extra beveiligingsniveau.

4.2 Containers

89% van de personen die hun eigen apparaat voor zakelijke doeleinden gebruiken, zegt op dit apparaat met essentiële bedrijfsgegevens te werken. 41% zegt zijn eigen apparaat zonder toestemming op het werk te gebruiken.[2]

Zelfs de voorzichtigste werknemers kunnen per ongeluk de bedrijfssystemen in gevaar brengen door bepaalde consumententoepassingen te downloaden of persoonlijke gegevens op het apparaat te openen.

Hier komt het werken met containers van pas. Dit is een eenvoudige oplossing waarmee persoonlijke en zakelijke content op het apparaat van elkaar wordt gescheiden. Hierdoor krijgt de IT-beheerder de volledige controle over bedrijfscontent en kan deze worden beschermd tegen alle risico's van privégebruik zonder privégegevens te beïnvloeden. Via containers kunnen IT-afdelingen beleidsregels voor beveiliging en gegevensbescherming toepassen op een 'zakelijke container' op een persoonlijk apparaat of een bedrijfsapparaat. Dit is met name nuttig voor BYOD-doeleinden.

4.3 Encryptie

Een best practice voor MDM moet ook de mogelijkheid bieden om gevoelige gegevens in de container te coderen. Encryptie verbetert de anti-diefstalstrategieën - forcering van gecodeerde gegevens leidt ertoe dat de gevolgen van het pas later wissen van een apparaat lang niet zo ingrijpend zijn.

Organisaties die instellen dat gegevens alleen gecodeerd in de zakelijke container op een apparaat kunnen worden opgeslagen, kunnen zich beschermen tegen gegevenslekken en kunnen naleving afdwingen rond gegevensbescherming. De MDM-encryptietechnologie van Kaspersky Lab kan worden geautomatiseerd en volledig transparant worden gemaakt voor de eindgebruiker, zodat uw beveiligingsbeleidsregels worden nageleefd.

4.4 Bescherming tegen diefstal en contentbeveiliging

Het is bijna onmogelijk kleine, ultra-mobiele apparaten fysiek te vergrendelen, maar u kunt de inhoud wel degelijk vergrendelen en bepalen wat er moet gebeuren als een apparaat zoekraakt.

De MDM-oplossing van Kaspersky Lab bevat mogelijkheden tegen diefstal en voor contentbeveiliging die op afstand zijn in te schakelen, zodat onbevoegden geen toegang krijgen tot gevoelige gegevens. Een greep uit de mogelijkheden:

2 Bron: Juniper Networks, Trusted Mobility Index 2012.

- **SIM-beheer:** een zoekgeraakte of gestolen telefoon vergrendelen, zelfs als de SIM-kaart is vervangen, en het nieuwe nummer naar de wettige eigenaar sturen.
- **Traceren locatie/apparaat:** via GPS, GSM of WiFi de locatie van een apparaat vaststellen.
- **Op afstand/selectief wissen:** Alle gegevens op een apparaat volledig wissen, of alleen gevoelige bedrijfsgegevens.
- **Op afstand vergrendelen:** onbevoegde toegang tot een apparaat voorkomen, zonder dat gegevens hoeven te worden gewist.

4.5 Mobiele anti-malware

U hebt een strategie nodig voor het omgaan met zoekgeraakte of gestolen apparaten. Apparaten lopen echter zelfs risico als ze in handen van geautoriseerde gebruikers zijn. Veel organisaties doen er alles aan om anti-malware- en anti-spamoplossingen in het bedrijfsnetwerk te implementeren, maar ondernemen slechts weinig om te voorkomen dat hun mobiele apparaten ten prooi vallen aan virussen of andere malware.

De technologieën van Kaspersky Lab voor mobiele beveiliging bevatten een gecombineerde anti-malwareoplossing met zowel signature-based detectie met pro-actieve, cloud-assisted technologieën. Dit verbetert detectieratio's en biedt realtime bescherming tegen malware. On-demand en geplande scans zorgen voor maximale beveiliging – automatische OTA-updates zijn essentieel voor elke MDM-strategie.

4.6 Houd het simpel: gecentraliseerd beheer

Met de technologieën van Kaspersky Lab kunnen beheerders mobiele apparaten beveiligen via dezelfde 'dashboardconsole' waarmee ze ook het netwerk en endpoints beveiligen. Dit neemt de complexiteit weg van afzonderlijke oplossingen en de bijbehorende verschillende, vaak incompatibele consoles. Door een wildgroei aan technologie wordt het geheel alleen maar complexer.

Door de beveiligingsconfiguratie voor meerdere apparaten te vereenvoudigen en te automatiseren, vermindert u niet alleen de last voor uw IT-medewerkers, maar verbetert u tevens mobiele beveiligingspraktijken. Nadat u uw beleidsregels eenmaal hebt vastgesteld, kunt u deze met één muisklik toepassen – of u nu tien apparaten onder uw beheer hebt of duizend.

4.7 Zoek de juiste balans

Het hoeft niet ingewikkeld of duur te zijn om uw mobiele IT-omgeving te implementeren, beheren en beveiligen. Met de MDM-oplossing van Kaspersky Lab wordt de veilige configuratie van mobiele apparaten eenvoudig en overzichtelijk. De mobiele agent die is geïnstalleerd op apparaten biedt alle bescherming tegen actuele dreigingen. Dit biedt IT-beheerders de zekerheid dat alle mobiele apparaten over de vereiste instellingen beschikken en beveiligd zijn als ze zoekraken, worden gestolen of worden misbruikt door de gebruiker.

Ongeacht de grootte van uw bedrijf is het van belang dat u uw mobiele apparaten op een juiste manier beheert, omdat ze anders een zware last gaan vormen voor de IT-afdeling, om nog maar te zwijgen over de beveiliging en het risico op gegevensverlies. Ongeacht of u de kosten wilt verlagen door een BYOD-initiatief te ondersteunen of door een strikt programma voor mobiele bedrijfsapparaten te hanteren, de risico's zijn uiteindelijk hetzelfde: steeds meer gegevens zitten bij medewerkers in hun broekzak, blijven achter in de taxi, worden gestolen of raken zoek.

Zou het niet geweldig zijn als de beveiliging en gegevensbescherming niet ten koste zouden gaan van uw mobiliteit, verbeterde productiviteit en eenvoud? Met Mobile Device Management (MDM) en geavanceerde mobiele beveiligingstechnologieën hoeft dat inderdaad niet.

4.5 Mobiele anti-malware

U hebt een strategie nodig voor het omgaan met zoekgeraakte of gestolen apparaten. Apparaten lopen echter zelfs risico als ze in handen van geautoriseerde gebruikers zijn. Veel organisaties doen er alles aan om anti-malware- en anti-spamoplossingen in het bedrijfsnetwerk te implementeren, maar ondernemen slechts weinig om te voorkomen dat hun mobiele apparaten ten prooi vallen aan virussen of andere malware.

De technologieën van Kaspersky Lab voor mobiele beveiliging bevatten een gecombineerde anti-malwareoplossing met zowel signature-based detectie met pro-actieve, cloud-assisted technologieën. Dit verbetert detectieratio's en biedt realtime bescherming tegen malware. On-demand en geplande scans zorgen voor maximale beveiliging – automatische OTA-updates zijn essentieel voor elke MDM-strategie.

4.6 Houd het simpel: gecentraliseerd beheer

Met de technologieën van Kaspersky Lab kunnen beheerders mobiele apparaten beveiligen via dezelfde 'dashboardconsole' waarmee ze ook het netwerk en endpoints beveiligen. Dit neemt de complexiteit weg van afzonderlijke oplossingen en de bijbehorende verschillende, vaak incompatibele consoles. Door een wildgroei aan technologie wordt het geheel alleen maar complexer.

Door de beveiligingsconfiguratie voor meerdere apparaten te vereenvoudigen en te automatiseren, vermindert u niet alleen de last voor uw IT-medewerkers, maar verbetert u tevens mobiele beveiligingspraktijken. Nadat u uw beleidsregels eenmaal hebt vastgesteld, kunt u deze met één muisklik toepassen – of u nu tien apparaten onder uw beheer hebt of duizend.

4.7 Zoek de juiste balans

Het hoeft niet ingewikkeld of duur te zijn om uw mobiele IT-omgeving te implementeren, beheren en beveiligen. Met de MDM-oplossing van Kaspersky Lab wordt de veilige configuratie van mobiele apparaten eenvoudig en overzichtelijk. De mobiele agent die is geïnstalleerd op apparaten biedt alle bescherming tegen actuele dreigingen. Dit biedt IT-beheerders de zekerheid dat alle mobiele apparaten over de vereiste instellingen beschikken en beveiligd zijn als ze zoekraken, worden gestolen of worden misbruikt door de gebruiker.

Ongeacht de grootte van uw bedrijf is het van belang dat u uw mobiele apparaten op een juiste manier beheert, omdat ze anders een zware last gaan vormen voor de IT-afdeling, om nog maar te zwijgen over de beveiliging en het risico op gegevensverlies. Ongeacht of u de kosten wilt verlagen door een BYOD-initiatief te ondersteunen of door een strikt programma voor mobiele bedrijfsapparaten te hanteren, de risico's zijn uiteindelijk hetzelfde: steeds meer gegevens zitten bij medewerkers in hun broekzak, blijven achter in de taxi, worden gestolen of raken zoek.

Zou het niet geweldig zijn als de beveiliging en gegevensbescherming niet ten koste zouden gaan van uw mobiliteit, verbeterde productiviteit en eenvoud? Met Mobile Device Management (MDM) en geavanceerde mobiele beveiligingstechnologieën hoeft dat inderdaad niet.

5. SAMENVATTING

Organisaties hebben niet alleen behoefte aan intelligente beveiligingstechnologieën om de gegevens te beveiligen, maar ook aan intuïtieve en niet te ingewikkelde IT-efficiëntietools. De 2500 medewerkers van Kaspersky Lab willen in deze behoeften voorzien voor de ruim 300 miljoen systemen die zij beveiligen en de 50.000 nieuwe systemen die daar dagelijks aan worden toegevoegd.

Kaspersky MDM is een onderdeel van Kaspersky Endpoint Security for Business. De zakelijke beveiligingsproducten van Kaspersky combineren bekroonde anti-malware, tools voor IT-beleidsnaleving, gecentraliseerd beheer en cloudgebaseerde beveiliging - de juiste keuze voor uw organisatie.

Neem contact op met uw IT-partner en informeer hoe Kaspersky kan zorgen voor een beveiligde configuratie van uw mobiele endpoint-implementatie.

Kaspersky Lab ZAO, Moskou, Rusland
www.kaspersky.nl