

Hvidbog

KASPERSKY<sup>lab</sup>

# Mobile sikkerhedsproblemer i erhvervsmiljøer

Be Ready for What's Next.

# Mobile sikkerhedsproblemer i erhvervsmiljøer

Markedet for smartphones vokser stærkt. Ifølge aktuelle beregninger foretaget af branchesammenslutningen BITKOM [1] vil det globale marked for it og kommunikation vokse med 4,8 procent i år. Mobile kommunikationsenheder - navnlig smartphones - er det hurtigst voksende område, og eksperter forventer en stigning i salget på hele 11,5 procent. Salget af smartphones har endog overhalet salget af pc'er, og enhederne bliver mere og mere populære til både erhvervsmæssig og privat brug.

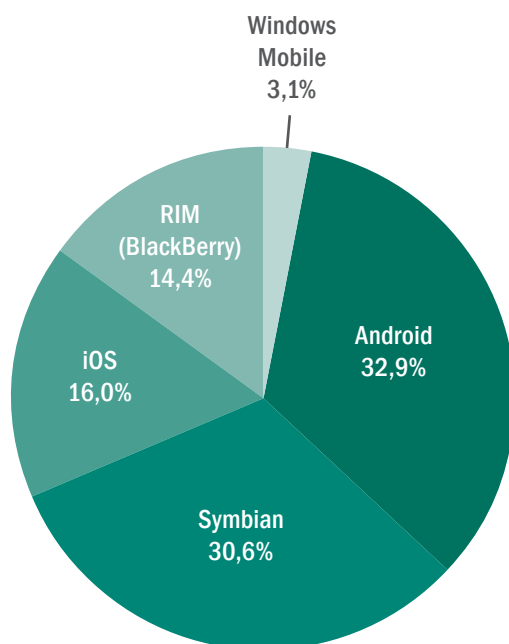
Dermed bliver virksomheder, som ikke nødvendigvis kræver, at deres medarbejdere bruger smartphones, forpligtet til at implementere dem til forretningsmæssige formål som følge af de ansattes brug af og personlige erfaringer med disse praktiske enheder. I mange virksomheder får medarbejderne også lov til at vælge deres egen enhed som frynsegode. European Information Technology Organisation (EITO) forventer et globalt salg på 1,4 milliarder mobiltelefoner i 2011.

## Det dynamiske smartphone-marked

Alle, der giver sig til at undersøge markedet for smartphones, vil bemærke, at der ikke i øjeblikket er et dominerende operativsystem, svarende til Windows på computerområdet. I stedet er der, som den seneste markedsanalyse fra Canaly [2] viser, flere udbydere med gode positioner, som hver får en pæn del af andelen af smartphone-markedet. Ved hjælp af et stort antal enheder over et bredt prisspektrum har Android-plattformen haft størst udbytte af den seneste vækst på markedet. Med 33,3 millioner Android-smartphones har Google opnået en markedsandel på 32,9 procent, hvilket giver dem den førende position på markedet. På andenpladsen finder man dog ikke Apple og deres allestedsnærværende iPhone. I stedet indtager Symbian med en markedsandel på 30,6 procent (31 millioner) pladsen lige bag Google og foran Apple. Først derefter kommer iPhones operativsystem iOS med 16,2 millioner enheder og en markedsandel på „kun“ 16 procent. Derefter kommer BlackBerry, som er meget populær blandt erhvervsbrugere, med en markedsandel på 14,4 procent. Til sidst finder vi Microsoft med deres nuværende Windows-operativsystem og en samlet markedsandel på 3,1 procent.

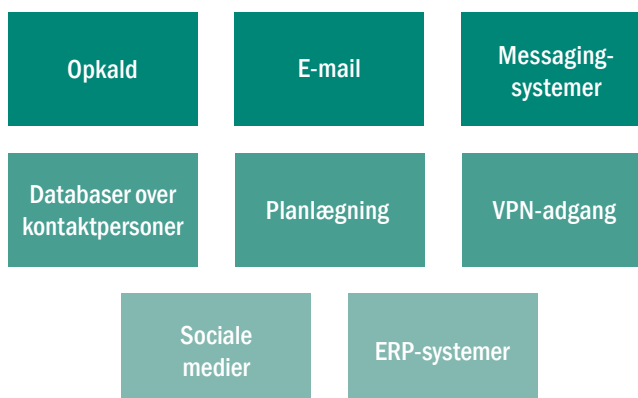
Markedet for smartphones udgør også en udfordring for analytikere, da det er særdeles vanskeligt at forudsige. For blot et år siden var iOS's markedsandel (16,3 procent) tilsvarende høj. Sidste år sad BlackBerry stadigvæk på en femtedel af markedet, mens Android, den nuværende nummer ét, lå sidst med 8,7 procent. Det lå dermed lige foran Windows Mobile, som dengang havde en markedsandel på 7,2 procent. For et år siden var Symbian stadigvæk nummer ét på markedet - og med en meget stor margen: 44,4 procent af markedsandelen.

Som en aktuel undersøgelse udført af Forbes Insights [3] viser, så er smartphonens andel af erhvervsmarkedet nu en helt anden. 87 af ledende medarbejdere i amerikanske virksomheder bruger laptop, og 82 bruger også smartphone. 28 procent har to enheder og ejer udover en BlackBerry, som er den klassiske enhed for erhvervsfolk, også en Android-baseret mobil enhed eller en iPhone. Smartphonen er den foretrukne kommunikationsenhed for mere end halvdelen af deltagerne i undersøgelsen.



### Det er nødvendigt at beskytte smartphonen

Og hvorfor skal virksomhederne så medtage smartphones i deres sikkerhedsstrategi? Den korte svar er, at smartphones bruges til mange formål. Det er derfor nødvendigt at beskytte disse mobile platforme. I virksomheder bruges smartphones især til at opnå adgang til kommunikationsplatforme, navnlig telefon- og e-mail-systemer, men de bliver i stadig højere grad også brugt til andre messaging-systemer, herunder planlægningssystemer. De bruges også til at få adgang til databaser over kontaktpersoner. I sådanne tilfælde er det vigtigt at sikre disse følsomme data. Tredjemand må ikke få adgang til virksomhedens e-mail, og de skal naturligvis heller ikke kunne få fat på oplysninger om kunder eller leverandører.



Det næste trin omfatter adgang til virksomhedens netværk. Medarbejderne bruger ofte en VPN-forbindelse til at koble sig på virksomhedens netværk, hvorfra de har adgang til filer og erhvervsapplikationer som f.eks. ERP-systemer (Enterprise Resource Planning). Det er vigtigt, at virksomhederne gennemfører tiltag, der forhindrer uvedkommende brugere i at få adgang til interne oplysninger i virksomheden, hentning af data eller manipulering af eksisterende programmer.

Det har i mange år været almindelig praksis, at virksomhederne har sikkerhedsstrategier for deres servere, arbejdsstationer og andre it-komponenter. Beskyttelse af smartphones, som bruges erhvervsmæssigt, udgør dog desværre stadigvæk ikke en fast bestanddel af virksomhedernes sikkerhedspolitik. Da der anvendes mange forskellige smartphones som beskrevet ovenfor, så vil det være klogt at beskytte virksomhedens smartphones.



### Den perfekte beskyttelsesstrategi

Der findes tre grundlæggende scenarier, som man bør beskytte smartphones imod. Den mest almindelige er Eksempel 1: bortkomst eller tyveri. Ifølge undersøgelser foretaget af BITKOM har 10 millioner tyskere allerede mistet en mobiltelefon [4], og i en nyere undersøgelse fra januar 2011 foretaget i 4 europæiske lande, der omfattede mobiltelefonbrugere fra 14 år og opad, fortalte 20 %, at de havde enten fået stjålet eller mistet deres mobiltelefon. Eksempel 2 minder om eksempel 1: andre personers fulde adgang til din mobiltelefon i et kortere tidsrum. Lad os bruge et populært eksempel: En medarbejder lader sin smartphone ligge på skrivebordet i frokostpausen, og en kollega eller tredjemand tager den op. Her er der også risiko for misbrug af virksomhedens oplysninger via uvedkommende adgang. Eksempel 3 er en kombination af alle de øvrige trusselscenarier – herunder malware specifikt udviklet til mobile enheder, sms-angreb og målrettet datatyveri ved hjælp af specialudviklede e-mail eller websteder. Det, der adskiller sig i dette tilfælde, er dog, at angriberne ikke har fysisk adgang til enheden.

Tab som følge af...	Uvedkommende adgang for...	Malware
<ul style="list-style-type: none"><li>• Tyveri</li><li>• Stress</li><li>• Glemsomhed</li><li>• Glemte telefon</li></ul>	<ul style="list-style-type: none"><li>• Kolleger</li><li>• Tredjemand</li><li>• Familienedlemmer</li></ul>	<ul style="list-style-type: none"><li>• Virus</li><li>• Sms-angreb</li><li>• Målrettet datatyveri</li></ul>

## Beskyt dig mod tab og tyveri

Hvis du taber eller får stjålet din smartphone, har tredjemand fysisk adgang til enheden. Hvis den bliver fundet af en uærlig person, har denne person nu ubegrænset tid til at få adgang på de data, der ligger på smartphonen. Ikke blot kan der ligge værdifulde data på selve den mobile enhed. Login-oplysninger til virksomhedens netværk eller kommunikationstjenester er også interessante. Hvis adgangskoder til VPN eller mailserever er gemt på telefonen, skal tyven blot aktivere den relevante applikation for at få adgang. Sikkerhedssoftware som Kaspersky Endpoint Security 8 for Smartphone har særlige tyversikringsfunktioner, der forhindrer uvedkommende i at få adgang til data på bortkomne enheder. Bortkomne smartphones kan også fjernblokeres ved hjælp af særlig administrationssoftware. Enheder med GPS-modtagere – en funktion der allerede er indbygget i de fleste smartphones til erhvervsbrug – kan også lokaliseres. Alternativt kan du anvende mere drastiske metoder og bruge en slettekommando til at gendanne enhedens fabriksindstillinger. Eftersom den bortkomne enhed alligevel skal erstattes, så er dette ikke et problem for de fleste virksomheder, og nulstillingen forhindrer, at følsomme informationer kommer i de forkerte hænder.

En professionel tyv vil hurtigt træffe de nødvendige foranstaltninger til at undgå at blive opdaget. Noget af det første, han eller hun vil gøre, er derfor at fjerne SIM-kortet. Her har Kaspersky Endpoint Security for Smartphones også en løsning: Funktionen SIM Watch gør det muligt for administrationssoftwaren at spore enheden, selvom SIM-kortet er fjernet. Selv det nye mobilnummer sendes automatisk pr. sms til telefonens retmæssige ejer.

Men hvad gør man, hvis smartphonen ikke kan låses i tide? I sådanne tilfælde er kryptering en fordel. Denne gennemprøvede metode har gennem årene vist sig at være effektiv til at beskytte data på laptops. Filer, mapper og lagringsmedier kan krypteres uigenkaldeligt ved hjælp af Kaspersky Endpoint Security, som sikrer, at kun personer med den rigtige adgangskode kan få adgang til dataene.

### Den perfekte sikkerhedssoftware til mobile enheder:

- Blokering af adgang
- Kryptering
- Beskyttelse af fortrolige oplysninger
- Fjernadministration
- Support af regler
- Support på flere platforme

Problemet med mobil malware undervurderes ofte. Tallet kan jo næppe sammenlignes med den aktuelle situation for Windows. Der findes malware for de forskellige mobile platforme, f.eks. trojanere, der sender sms'er til premiumtjenester for at skabe enorme regninger til telefonens ejer, men der har til dato har kun været få større virusudbrud. Man bør dog være forsigtig, da smartphones og tablet-computere bliver mere og mere populære og dermed interessante mål for skabere af malware. Det bør også bemærkes, at ikke alle virusangreb nødvendigvis har til formål at skabe mediesensationer. Sikkerhedsekspertter har observeret, at malware gennem en del år er blevet mere og mere professionel. Kvalitet kommer før kvantitet, og hvis nogen er interesseret i dataene på dine sælgeres smartphones, så udgør et målrettet angreb en stor risiko. Vi anbefaler, at du træffer forholdsregler i form af beskyttelse mod mobilvirus. Kaspersky Endpoint Security 8 for Smartphone beskytter mobile enheder i realtid og udfører planlagt malwarekontrol af hele enheder. Dette kan forhindre, at datatyvene får et forspring og dermed forhindre store trusler. Ud over en løsning til mobil beskyttelse er et spamfilter også vigtigt. Dets funktioner bør ikke være begrænset til e-mail. Det bør også filtrere uønskede sms'er og opkald.

### Yderligere sikkerhedstiltag

Adgangsblokering og kryptering bidrager til at skjule oplysninger, men avanceret sikkerhedssoftware kan mere endnu, blandt andet beskytte fortrolige oplysninger. Med Kaspersky Endpoint Security 8 for Smartphone kan brugerne eksempelvis skjule enkelte kontaktpersoner, opkaldslistor og sms'er.

### Enkel sikkerhed til smartphones

Smartphones kan en helt masse, og de påvirkes af mange forskellige trusler. Heldigvis er det meget nemt at beskytte disse alsidige mobile enheder. Når virksomhederne vælger sikkerhedssoftware til smartphones, bør følgende overvejes.

### Administrationsfunktioner

Det er meget nemt at konfigurere én smartphone manuelt. Konfiguration af fem eller flere kan dog være besværligt, og konfiguration af mere end 10 er uøkonomisk uden et centralt administrationsinterface med adgang til vedligeholdelse af mobile enheder. Og det er lige nøjagtig, hvad Kaspersky Endpoint Security 8 for Smartphone kan. Eftersom administrationen også kan fjernstyres, har it-teamet fuld kontrol over enhederne altid. Det gør det muligt at udføre opdateringer og at installere nye programmer nemt og målrettet. Når du vælger en mobil sikkerhedssuite, skal du også være opmærksom på, at Kaspersky Endpoint Security ud over administration via Kaspersky Administration Kit også kan integreres fuldt ud med eksisterende administrationsmiljøer til mobile enheder, f.eks. fra Microsofts Mobile Device Manager og Sybase Afaria.

## Regler

Hvem kan gøre hvad i netværket? Regler er blevet uundværlige for virksomhederne, og ikke kun af hensyn til overholdelse af lovgivning. De er også nødvendige, for at der kan foretages en fuld og sikker integration af smartphones. Kaspersky Endpoint Security tillader derfor, at der kan defineres regler for forskellige brugergrupper - fjernstyret naturligvis. Det gør det nemt for administratorene at justere telefonernes indstillinger for antivirus og eksempelvis definere, hvilke filtyper der skal scannes for malware, og hvilke der ikke skal. Desuden kan tyverisikringen naturligvis konfigureres til et meget detaljeret niveau. Vil du foretage fjernstyret sletning af indholdet på stjalne smartphones? Du kan definere regler, så det er muligt. It-teamet har også fuld kontrol, når det gælder kryptering. Regler bruges til at definere, hvilke mapper der skal krypteres. En anden fordel er, at medarbejderne ikke behøver foretage sig noget. Deres smartphones konfigureres automatisk. Resultatet bliver, at administratorene sparer enorme mængder tid og dermed penge. Ved brug af denne metode er det ikke nødvendigt at indsamle smartphones og docke dem med en pc eller løbende oprette forbindelse til virksomhedens netværk for at foretage justeringer af sikkerhedsindstillingerne.

## Beskyttelse af alle platforme

Gå ikke på kompromis, når det gælder sikkerhed for smartphones. Den sikkerhedssoftware, du vælger, skal understøtte alle de mobile platforme, virksomheden anvender. Kaspersky Endpoint Security 8 for Smartphone understøtter BlackBerry-, Windows Mobile-, Android- og Symbian-enheder. Kort sagt: Kaspersky Lab-løsningen dækker med andre ord ca. 85 procent af smartphone-markedet. Eftersom Kaspersky Labs sikkerhedsløsninger kræver meget få ressourcer, er der ingen negativ effekt på de mobile enheders ydeevne.

## Om Kaspersky Lab

Det er vores holdning, at alle skal kunne udnytte teknologien bedst muligt uden frygt for indtrængen eller andre sikkerhedsproblemer. Vores team af specialister giver dig frihed til at leve dit digitale liv uden at skulle bekymre dig om dine personlige data og penge.

I 13 år har vi arbejdet på at eksponere, analysere og neutralisere it-trusler. Undervejs har vi samlet enorme mængder erfaring og viden om malware og håndteringen af den. I dag har Kaspersky Lab en fast position som én af verdens fire største leverandører af software til endpointbrugere.

Kaspersky Lab er en international koncern med over 2.000 højtuddannede specialister og centralt hovedkvarter i Moskva samt regionale hovedkvarterer, der styrer aktiviteterne hos lokale repræsentanter og samarbejdspartnere i fem globale regioner: Vesteuropa, Østeuropa, Mellemøsten og Afrika, Nord- og Sydamerika, Asien-Stillehavet og Japan. Virksomheden har i øjeblikket aktiviteter i over 100 lande over hele verden og egne afdelinger i 27 lande. Virksomhedens produkter og teknologier beskytter 300 millioner brugere over hele verden. Koncernens vigtigste beslutningstagende enhed er bestyrelsen, som er ansvarlig for den samlede udviklingsstrategi samt udpegning af den øverste ledelse. Bestyrelsen består af ni aktionærer og topledere, der repræsenterer det centrale hovedkvarter og de globale regioner.

Over 300 millioner mennesker over hele verden er beskyttet af Kaspersky Labs produkter og teknologier, herunder brugere af tredjepartsprodukter, der omfatter Kaspersky Labs Anti-Virus Engine. Kaspersky Labs klientgrundlag for hele koncernen omfatter over 200.000 virksomheder over hele verden fra små og mellemstore virksomheder og op til store statslige og kommercielle organisationer.

Kaspersky Labs kundetal vokser dag for dag, og i øjeblikket har vi over 10 millioner produktaktiveringer om måneden.

## Kaspersky Endpoint Security for Smartphone

Kaspersky Endpoint Security for Smartphone er en ny applikation i en produktserie, der er baseret på et ensartet sæt anti-malware-programmer og andre kerneteknologier i verdensklasse. Den yder brugervenlig sikkerhed, som er nem at administrere, og som beskytter fortrolige data på virksomheders mobile enheder mod tab, tyveri, uvedkommende adgang og malware, uanset hvor dine medarbejdere færdes.

### Vigtige egenskaber

#### Robust beskyttelse af data

Kaspersky Endpoint Security for Smartphone tilbyder effektive sikkerhedsfunktioner som kryptering, antivirus, firewall, spamfilter til tale og sms og beskyttelse af fortrolige oplysninger samt tyverisikring med fjernstyret lås/sletning og GPS-sporing.

#### Support på flere platforme

Applikationen yder effektiv anti-malware-beskyttelse til mobile enheder, der kører på mobiltelefoner med Symbian S60, Black-Berry, Android og Windows Mobile.

#### Nem aktivering

Du kan nemt aktivere Kaspersky Endpoint Security for Smartphone fra ét punkt til alle mobile enheder i virksomheden, enten trådløst eller ved at tilslutte smartphonen til en pc.

#### Effektiv administration

Med applikationen kan systemadministratorer håndtere indstillinger, begrænsninger, koncernregler m.m. fra en central konsol ved hjælp af Kaspersky Administration Kit, Sybase Afaria eller Microsoft System Center Mobile Device Manager.

### Systemkrav

#### Understøttede administrationsplatforme:

- Kaspersky Administration Kit 8.0 (version 8.0.2121 eller senere)
- Microsoft System Center Mobile Device Manager 2008 SP1
- Sybase Afaria 6.5

#### Understøttede operativsystemer:

- Symbian S60 9.1-9.4 (kun Nokia)
- Windows Mobile 5.0-6.5
- BlackBerry 4.5-5.0
- Android 1.5-2.3

[1] [www.BITKOM.org/66938\\_66928.aspx](http://www.BITKOM.org/66938_66928.aspx)

[2] [www.canalys.com/pr/2011/r2011013.html](http://www.canalys.com/pr/2011/r2011013.html)

[3] [http://images.forbes.com/forbesinsights/StudyPDFs/The\\_Untethered\\_Executive.pdf](http://images.forbes.com/forbesinsights/StudyPDFs/The_Untethered_Executive.pdf)

[4] [www.BITKOM.org/de/presse/66442\\_64952.aspx](http://www.BITKOM.org/de/presse/66442_64952.aspx)

Kaspersky Lab  
Automatikvej 1  
2860 Soeborg  
Denmark

(866) 477-0347  
[corporatesales@kaspersky.dk](mailto:corporatesales@kaspersky.dk)

[www.kaspersky.dk](http://www.kaspersky.dk)  
[www.securelist.com](http://www.securelist.com)  
[www.threatpost.com](http://www.threatpost.com)