Whitepaper

KASPERSKY lab

Tekniskt dokument
Säkerhetsfrågor kring mobilitet i företagsmiljöer

Be Ready for What's Next.

Säkerhetsfrågor kring mobilitet i företagsmiljöer

Marknaden för smartphones har haft en mycket stark utveckling. Enligt nyligen gjorda uppskattningar av branschorganisationen BITKOM [1] kommer den globala marknaden för IT och kommunikation att växa med 4,8 procent det här året. Mobil kommunikationsutrustning och i synnerhet smartphones går i bräschen för den här utvecklingen och branschexperter förutser en försäljningsökning på uppemot 11,5 procent i det aktuella marknadssegmentet. Försäljningen av smartphones överstiger nu försäljningen av persondatorer, och de här produkterna blir allt mer populära bland både företags- och hemanvändare.

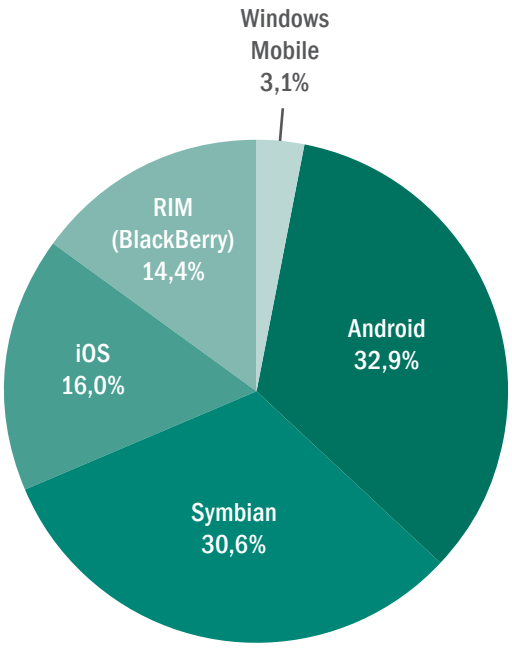
Ett resultat av utvecklingen är att även företag som själva inte kräver att personalen använder smartphones tvingas att införa dem i systemen, på grund av de anställdas personliga och praktiska erfarenheter. På många företag har de anställda även möjligheten att själva välja vilken typ av enhet de ska använda. Enligt prognoser från EITO (European Information Technology Organisation) kommer närmare 1,4 miljarder mobiltelefoner att säljas under 2011.

Den dynamiska marknaden för datormobiler

Alla som tittar närmare på marknaden för smartphones kommer att upptäcka att det idag inte finns något operativsystem som dominerar på samma sätt som Windows gör på persondatormarknaden.
I stället har flera leverantörer bra positioner på marknaden med stabila marknadsandelar, något som bland annat visas av Canalys senaste marknadsanalys [2]. Tack vare ett stort antal modeller i flera prissegment har plattformen Andriod tjänat mest på den senaste tidens marknadsexpansion. Med 33,3 miljoner Android-telefoner har Google nått en marknadsandel på 32,9 procent vilket gör företaget till marknadens ledande tillverkare. På andra plats ligger inte Apple med succén iPhone, utan operativsystemet Symbian med 30,6 procent av marknaden (vilket motsvarar 31 miljoner enheter) och ett ordentligt försprång framför Apple. Därefter kommer iPhone-operativsystemet iOS med drygt 16,2 miljoner enheter och en marknadsandel på ”bara” 16 procent. Sedan kommer BlackBerry, som är mycket populärt bland företagsanvändare i USA med en marknadsandel på 14,4 procent. Längst bak i fältet finns Microsoft med den mobila versionen av operativsystemet Windows och en total marknadsandel på 3,1 procent.

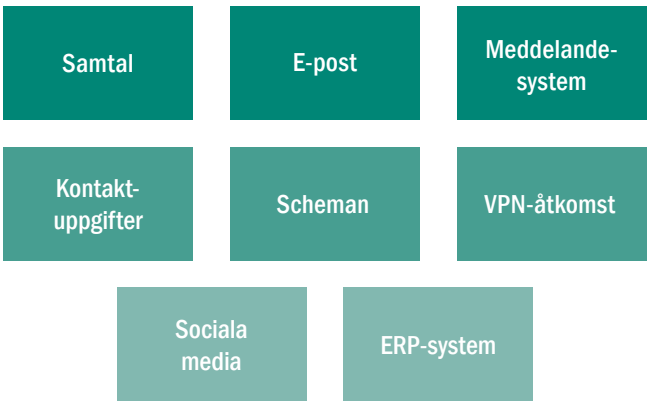
Marknaden för smartphones innebär också en utmaning för analytiker eftersom det är extremt svårt att göra hållbara prognoser. För ett år sedan var marknadsandelen för iOS (16,3 procent) lika hög som idag. BlackBerry hade femteplatsen på marknaden, och dagens marknadsledare Android höll sig i bakgrunden med 8,7 procent. Därmed låg man ett steg före Windows Mobile, som då hade 7,2 procent av marknaden. För ett år sedan var Symbian fortfarande marknadsledande – och detta med ordentlig marginal och en marknadsandel på 44,4 procent.

En nyligen genomförd studie av Forbes Insights [3] visar att smartphones andel av företagsmarknaden idag ser helt annorlunda ut. 87 procent av personal på ledande befattningar i USA använder bärbara datorer, och 82 procent använder dessutom en datormobil eller smartphone. 28 procent är ”dubbelanvändare”, vilket betyder att de förutom den klassiska företagsenheten BlackBerry också använder en Android-baserad mobiltelefon eller en iPhone. Smartphones är det primära kommunikationsverktyget för fler än hälften av de tillfrågade.



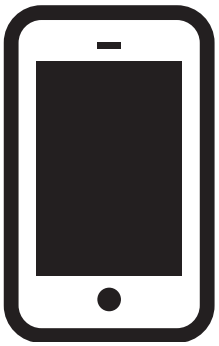
Alla datormobiler måste skyddas

Varför ska företag ta med smartphones i sina säkerhetsstrategier? Det enkla svaret på den frågan är att smartphones har många användningsområden vilket gör det viktigare att skydda de här mobila plattformarna. På företag används smartphones mest för åtkomst till kommunikationsnätverk – primärt telefoni- och e-postsystem, men också i allt högre utsträckning andra meddelandesystem, till exempel projektlednings- och schemaläggningssystem. De används också i hög grad för åtkomst till databaser med kontaktinformation. I samtliga dessa fall måste konfidentiell företagsinformation skyddas. Utomstående ska inte kunna ha tillgång till företagets e-postkorrespondens, och naturligtvis ska de inte heller kunna komma åt kund- eller leverantörsuppgifter.



Nästa steg handlar om åtkomsten till företagets interna nätverk. Anställda använder vanligtvis en VPN-anslutning för att komma åt företagets interna nätverk och därifrån kan de arbeta med dokument och affärssystem som till exempel ERP-lösningar (Enterprise Resource Planning). Här är det viktigt att företag vidtar åtgärder som förhindrar att utomstående kommer åt intern företagsinformation, samlar in data eller manipulerar befintliga applikationer.

Under många år har det varit vanligt att företag har en säkerhetspolicy som täcker servrar, arbetsstationer och andra IT-komponenter. Att skydda smartphones som används i företagssammanhang är tyvärr ännu inte en självklar del i företagets säkerhetspolicy. Med tanke på de många användningsområdena för smartphones är det ett klokt steg att skydda ditt företags smartphones.



Den perfekta skyddsstrategin

Detta är de grundläggande scenarier som datormobiler måste skyddas mot. Det allra vanligaste är: Fall 1: stöld eller förlust. Enligt undersökningar som utförts av BITKOM har 10 miljoner tyskar redan blivit av med minst en mobiltelefon [4] och i en nyligen utförd studie från januari 2011 i fyra europeiska länder som riktade sig mot mobilanvändare från 14 års ålder, har 20 % av de tillfrågade svarat att de hade tappat bort eller blivit bestulna på sina mobiltelefoner.Fall 2 påminner om fall 1: någon annan har fullständig åtkomst till din mobila enhet under en begränsad tid. Ett vanligt exempel är att en anställd låter sin datormobil ligga kvar på skrivbordet när han går på lunch, och en kollega eller utomstående tar upp telefonen. Här finns det också en reell risk för missbruk av företagsinformation genom obehörig åtkomst.Fall 3 är en kombination av alla andra hotscenarier, inklusive virus som är specialskrivna för mobila enheter, SMS-attacker och riktade dataintrång med särskilt konstruerade e-postmeddelanden eller webbplatser. Det som gör det här fallet annorlunda är att angriparen inte har fysisk åtkomst till enheten.

Förluster på grund av...	Obehörig åtkomst på grund av...	Sabotageprogram
• stöld • stress • glömska • telefonen glöms kvar	• kolleger • utomstående • familjemedlemmar	• virus • SMS-attacker • riktade dataintrång

Att skydda sig mot stöld och förlust

Om din datormobil blir stulen eller försvinner kan en utomstående få fysisk åtkomst till din enhet. Är den som hittar mobilen en oärlig person har han eller hon nu all tid i världen att ta sig in i den information som finns lagrad på datormobilen. Det som kan vara intressant för en kriminell person handlar inte bara om den information som finns lagrad på själva enheten utan också om inloggningsuppgifter till företagets nätverk eller kommunikationstjänster. Om lösenord till VPN-konton eller e-postservrar också finns i telefonen behöver tjuven bara starta rätt program för att få full åtkomst. Skyddsprogramvara som Kaspersky Endpoint Security 8 for Smartphones innehåller särskilda stöldskyddsfunktioner som förhindrar att utomstående kommer åt information på stulna eller försvunna datormobiler. En smartphone som har försvunnit kan till och med spärras med en särskild fjärrhanteringsprogramvara. Enheter med GPS-mottagare – en funktion som finns i de flesta moderna mobiltelefoner – kan också spåras och identifieras. Ett radikalt alternativ är att använda ett raderingskommando och göra en fullständig fabriksåterställning av enheten. Även om den försvunna enheten måste ersättas, innebär detta inte ett problem för de flesta företag, och en återställning innebär att känsliga företagsdata inte riskerar att falla i orätta händer.

En professionell tjuv vidtar snabbt åtgärder som syftar till att undgå upptäckt. En av de första saker han eller hon gör är att ta bort SIM-kortet ur den stulna telefonen. Här har Kaspersky Endpoint Security for Smartphones också en lösning – funktionen SIM Watch aktiverar en hanteringsprogramvara som spårar enheten, även om SIM-kortet tas bort. Det nya mobilnumret skickas till och med via SMS till telefonens rättmätige ägare.

Men vad händer om det inte går att låsa datormobilen i tid? I den här situationen träder krypteringen i kraft. Den här beprövade metoden har under lång tid visat sig vara effektiv när det gäller att skydda data på bärbara datorer. Filer, mappar och lagringsmedia kan permanentkrypteras med Kaspersky Endpoint Security, vilket garanterar att endast den med rätt lösenord kan komma åt informationen.

Den perfekta programvarulösningen för skydd av mobila enheter bygger på

- åtkomstspärr
- kryptering
- sekretesskydd
- fjärradministration
- stöd för regler
- stöd för flera plattformar

Hotet från sabotageprogramvara som riktas mot mobila plattformar är ett problem som ofta avfärdas. Trots allt kan omfattningen inte jämföras med den aktuella situationen för Windows. Även om det existerar skadlig programvara för mobila plattformar, till exempel trojaner som skickar SMS till betaltjänster och ger ägaren enorma telefonräkningar har det än så länge bara förekommit ett fåtal större virusutbrott. Däremot bör man vara uppmärksam eftersom den ökande andelen datormobiler och pekplattor har gjort mobila lösningar till intressant mål för upphovsmännen bakom skadlig programvara. Det kan också nämnas att alla virusangrepp inte syftar till att skapa uppmärksamhet i media. Säkerhetsexperter har identifierat en allt större professionalism i den värld där skadlig programvara framställs. Kvalitet börjar bli viktigare än kvantitet, och om någon är intresserad av den information som finns i ditt säljteams datormobiler är ett riktat angrepp en ytterst reell risk. Vårt råd är att vidta skyddsåtgärder mot mobila virus. Kaspersky Endpoint Security 8 for Smartphone skyddar mobila enheter i realtid och utför schemalagda kontroller av skadlig programvara för hela enheten. Detta kan förhindra att datatjuven får ett försprång, och stora och allvarliga hot kan stävjas innan de får riktigt genomslag. Förutom ett skydd för mobila enhete, är en skyddsmodul för skräppost ett viktigt verktyg. Funktionaliteten är inte begränsad till e-postmeddelanden utan kan också filtrera bort oönskade samtal och SMS.

Ytterligare säkerhetsåtgärder

Även om åtkomstspärrar och kryptering hjälper till att dölja informationen har sofistikerade skyddsprogram även andra metoder på repertoaren, till exempel funktioner för sekretesskydd. Med Kaspersky Endpoint Security 8 for Smartphone kan användaren till exempel dölja individuella kontakter, samtalslistor och SMS-meddelanden.

Enkel säkerhet för smartphones

En smartphone kan göra många saker och de hot de ställs inför ser väldigt olika ut. Lyckligtvis är det mycket enkelt att skydda de här mobila allroundverktygen. När du väljer mellan säkerhetsprogram för smartphones bör du ta följande punkter i beaktande.

Administrativa funktioner

Det är enkelt att konfigurera en ensam smartphone manuellt. Att konfigurera fem eller fler kan vara tidsödande och att konfigurera fler än 10 är oekonomiskt utan en centraliserad administrationsinfrastruktur som kan användas för direkt åtkomst till de mobila enheterna. Detta är precis vad Kaspersky Endpoint Security 8 for Smartphone gör. Eftersom administrationen kan skötas från en fjärransluten dator har IT-avdelningen kontinuerligt total kontroll över enheterna. Detta gör att nya program och uppdateringar kan installeras snabbt och enkelt på de enheter där uppdateringarna verkligen behövs. När du väljer en lösning för mobil säkerhet ska du också tänka på att Kaspersky Endpoint Security inte bara kan styras via Kaspersky Administration Kit utan också kan integreras skarvlöst i befintliga administrativa miljöer, till exempel Microsofts hanteringssystem för mobila enheter, eller Sybase Afaria.

Regler

Vem kan göra vad i ditt nätverk? Säkerhetspolicies har blivit oumbärliga verktyg för företag och det handlar inte bara om att efterfölja standarder och myndighetsdirektiv. De är däremot ett måste för en enkel och säker integrering av smartphones i verksamheten. I Kaspersky Endpoint Security finns därför regler som kan kopplas till olika användargrupper – självklart i realtid från en central plats. Den här metoden gör att administratören enkelt kan justera datormobilens virusskydd, och till exempel definiera vilka filtyper som ska genomsökas efter skadlig programvara och vilka som kan släppas igenom. Naturligtvis kan stöldskyddsfunktionerna konfigureras på en mycket detaljerad nivå. Vill du radera innehållet på en stulen datormobil utan att ha tillgång till mobilen fysiskt? Du kan definiera regler som tillåter dig att göra detta. Också när det gäller kryptering har IT-avdelningen fullständig kontroll. Regler används för att definiera vilka mappar som måste krypteras. En annan fördel är att de anställda inte behöver göra någonting. Deras smartphones är automatiskt konfigurerade på exakt rätt sätt. Till slut handlar det om att administratörer kan spara mycket tid och därigenom mycket pengar. Att använda den här metoden eliminerar trots allt behovet av att samla in datormobilerna fysiskt, docka dem med en dator eller att ha dem kontinuerligt anslutna till företagets interna nätverk så att säkerhetsinställningarna kan justeras.

Skydd för alla plattformar

När det gäller säkerhet för datormobiler finns det ingen anledning att kompromissa. De skyddsprogram du väljer måste kunna hantera alla mobila plattformar som används inom företaget. Kaspersky Endpoint Security 8 for Smartphone har i dagsläget stöd för BlackBerry, Windows Mobile, Android och Symbian. Det innebär att lösningen från Kaspersky Lab täcker omkring 85 procent av marknaden. Eftersom säkerhetslösningarna från Kaspersky Lab är så resurssnåla har de ingen negativ påverkan på de mobila enheternas prestanda.

Om Kaspersky Lab

Vi tror att alla ska ges möjlighet att utnyttja tekniken maximalt – utan intrång eller andra säkerhetsproblem. Vårt specialistteam består av experter som ger dig möjlighet att leva ditt digitala liv utan att behöva oroa dig för din personliga information och dina personliga resurser.

Vi har under 13 års tid arbetat med att exponera, analysera och neutralisera IT-hot. Genom åren har vi skapat en enorm erfarenhets- och kunskapsbas kring skadlig programvara och hur den kan hanteras. Idag har Kaspersky Lab en stabil position som ett av världens fyra ledande IT-säkerhetsföretag för slutanvändare.

Kaspersky Lab är ett internationellt företag med över 2 000 högt kvalificerade specialister. Huvudkontoret ligger i Moskva och företaget har regionala centra som övervakar lokala representanter och samarbetspartners i fem globala regioner: Västeuropa, Österuropa, Mellanöstern och Afrika, Nord- och Sydamerika, samt Asien och Japan. Företaget driver verksamhet i över 100 länder och har egna lokalkontor i 27 länder. Företagets produkter och tjänster skyddar över 300 miljoner användare över hela världen. Företagets ledning består av styrelsen, som ansvarar för att skapa en övergripande strategi och för att utse ledande befattningshavare. Styrelsen består av nio aktieägare och anställda i ledande ställning från huvudkontoret och de globala regionerna.

Över 300 miljoner människor över hela världen skyddas av produkter och tjänster från Kaspersky Lab, inklusive användare av tredjepartslöningar som bygger på Kaspersky Lab Anti-Virus Engine. Kaspersky Lab har en kundbas som består av fler än 200 000 företaget över hela världen, från små och medelstora företag till myndigheter och multinationella företag.

Antalet kunder hos Kaspersky Lab växer varje dag, och fler än 10 miljoner produkter aktiveras varje månad.

Kaspersky Endpoint Security for Smartphone

Kaspersky Endpoint Security for Smartphone är en ny programvarulösning i en produktfamilj som bygger på en gemensam, marknadsledande kärna av tekniker för skydd mot skadlig programvara. Den ger dig en lättanvänd och lätthanterad säkerhetslösning som skyddar känslig information på företagets mobila enheter mot stöld, förlust, obehörigt användande och skadlig programvara, oavsett var dina anställda befinner dig.

I fokus

Garanterar robust dataskydd

Kaspersky Endpoint Security for Smartphone innehåller flera centrala säkerhetsfunktioner som kryptering, virusskydd, brandvägg, skräppostskydd för samtal och SMS, sekretesskydd, och dessutom stöldskydd med fjärråterställning och GPS-spårning.

Stöd för flera plattformar

Programmet ger effektivt skydd mot skadlig programvara på mobila enheter med Symbian S60, BlackBerry, Android och Windows Mobile.

Enkel distribution

Du kan utan problem rulla ut Kaspersky Endpoint Security for Smartphone från en central punkt till företagets alla mobila enheter, antingen över radiolänk eller när datormobilerna är anslutna till en persondator.

Effektiv administration

Med programmet kan systemadministratörer hantera inställningar, restriktioner, grupprinciper och mycket annat från en centraliserad konsol med Kaspersky Security Center, Sybase Afaria eller Microsoft System Center Mobile Device Manager.

Systemkrav

Aministrationsplattformar som stöds:

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

Operativsystem som stöds:

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

[1] www.BITKOM.org/66938_66928.aspx
[2] www.canalys.com/pr/2011/r2011013.html
[3] http://images.forbes.com/forbesinsights/StudyPDFs/The_Untethered_Executive.pdf
[4] www.BITKOM.org/de/presse/66442_64952.aspx

Kaspersky Lab AB
Färögatan 33
164 51 Kista
Sweden

+46 8 5785 3000
corporatesales@kaspersky.se

www.kaspersky.se
www.securelist.com
www.threatpost.com

b5ya