Whitepaper

KASPERSKY lab

Den verkliga kostnaden för säkerhet
Fem sätt som ditt antivirusskydd dränerar din budget på

Be Ready for What's Next.

Den verkliga kostnaden för säkerhet: Fem sätt som ditt antivirusskydd dränerar din budget

IT-miljön blir allt mer komplex och hoten från skadliga program allt allvarligare. IT-ansvariga på företagen tvingas att omvärdera sina antiviruslösningar då lösningar som fungerade igår idag är ineffektiva. I dagens hotbild ingår mobila plattformar, open source-operativsystem och Internet. Antivirusprogram är inte som tidigare en produktinvestering och företagen upptäcker att deras aktuella lösningar förorsakar kostnader som de aldrig hade kunnat föreställa sig. När du börjar fundera över att förnya eller byta ut nuvarande lösning rekommenderar Kaspersky Lab ett nytt synsätt på antiviruslösningar. Vi kallar detta synsätt Den verkliga kostnaden för säkerhet.

Dagens IT-miljö

Dagens IT-miljö kännetecknas av komplexitet och förändring. Nätverksgränserna är inte längre tydliga och användarna ansluter sig i allt större utsträckning till företagets resurser via publika nätverk med smartmobiler, bärbara datorer och surfplattor. Säkerhet på användarnivå blir normen när företagspolicyn att använda användarägd utrustning breder ut sig. Data är inte längre inlåsta i huvuddatorn eller servern utan finns istället på ett antal företags- och privatägda enheter. Användningen av open source och andra operativsystem än Microsoft skapar en allt mångsidigare operativsystemmiljö. Virtualisering och molnbaserad datoranvändning ritar om kartan för IT-administratörerna och medför ytterligare säkerhetsproblem.

Detta tumult av tekniska förändringar väcker nya, spännande möjligheter för företag och IT men öppnar även nya dörrar för cyberbrottsligheten. Samtidigt håller säkerhetsexperter på att bli en försvinnande liten skara och budgetarna krymper.

Enligt Frost & Sullivan är personalkostnaderna inom informationssäkerhet under 2011 i många länder lika stora som under 2008. Betänk då följande: I tre år har antalet attackvägar och hot från skadlig programvara ökat exponentiellt medan säkerhetspersonalens storlek har varit konstant. I och med att tekniken förändras och hoten från skadliga program eskalerar är bara det faktum att ha lika stora personalresurser för att hantera hoten en utmaning. Ofta reagerar IT-avdelningarna på förändringar och bedömer risker först efter att nya tekniker som t.ex. sociala nätverksprogram och mobila enheter har kommit i allmänt bruk. I andra situationer börjar IT-avdelningarna använda ny teknik innan säkerhetspersonalen har fått den kunskap som behövs för att skydda miljön. Så är t.ex. fallet med molnbaserad datoranvändning.(1) Företagen utvecklas snabbare än deras säkerhetspersonal klarar av och inga ansträngningar görs för att kompensera för brister i säkerhetstänkandet.(2)

Under tiden utvecklas även de skadliga programmen. Virus, maskar, spionprogram, phishing - dessa hot dyker ständigt upp och risken som de utgör blir större och större. Det handlar inte längre om en datanörd som sitter och skriver skript på sin kammare utan dagens skapare av skadliga program har ekonomiska motiv. De är ute efter känslig och hemlig data - data vars förlust kan få företagen på knä i form av advokatkostnader och skadeståndsprocesser, skadad goodwill och misstro från kunderna. Trots år av säkerhets- och teknikutveckling brottas vi fortfarande med skadliga program och de som attackerar är inte underbemannade, utarbetade eller underkvalificerade. De utvecklar ständigt sin taktik att utnyttja sårbarheter i sociala medier, mobila enheter, virtualiserade miljöer eller molnet. De största hot som säkerhetsproffsen oroar sig för enligt rapporter från Frost & Sullivan är sårbarheten hos program (73 %), mobila enheter (66 %) samt virus- och maskattacker (65 %). Det är värt att notera att samtidigt som virus- och maskattacker rankas som trea spelar dessa en viktig roll även när det gäller sårbarheten i program och hoten via mobila enheter.

Dagens antivirusskydd

Antiviruslösningarna som fungerade förr passar inte in i dagens IT-miljö. Signaturbaserat antivirusskydd vid gatewayen för e-post missar zero-day-attacker, rootkits, botnets, drive-by-nedladdningar, spyware osv. Dagens IT-infrastruktur kräver en avancerad antiviruslösning från en stark leverantör som skyddar hela och den ständigt föränderliga IT-miljön. Företagen behöver investera i ett antivirusföretag och inte bara i en produkt.

”Det är forskning och support som är avgörande för hur bra ett antivirusprogram är. Det avgörande är snabba svarstider på nya hot och förstklassig assistans till kunderna. När fokus i företagens nätverk skiftar från stationära datorer till bärbart, moln och virtuell datormiljö behöver säkerhetsprogrammen skydda även dessa miljöer”, säger Lysa Myers, forskningsansvarig på West Coast Labs i en rapport som beskriver den förändrade hotbilden (Changing Malware Threats in Corporate Networks).

Att hitta en ”framtidssäker” lösning är inte en dröm det kräver bara en djupare förståelse för valet av leverantör. Säkerhetsföretagen måste vara förutseende och även kunna möta hot som följer med ny teknik. Har leverantören ett forskningsteam som kan sätta fingret på framtida hot och attackvägar? Har de resurser att hålla sig steget före cyberbrottslingarna? ”I bedömningen av en produkts duglighet i företagets nätverksmiljö är ’skydd’ mer än bara aktuella möjligheter att upptäcka skadliga program, det handlar även om leverantörens produktresearch och utvecklingsstrategier för att uppfatta hot och trender. Helt enkelt kunna skydda nätverket förebyggande”, säger Myers.

Vad betyder det då? Regel 1: Antiviruslösningarna är inte längre desamma - de är ingen produktinvestering. Du kan inte få och kommer inte heller att kunna få ett kontinuerligt och robust skydd med någon gratisprodukt. Kommersiella leverantörer investerar också olika mycket på forskning och support den dyraste lösningen ger inte nödvändigtvis ett kontinuerligt och robust skydd. Med detta i åtanke krävs det ett nytt synsätt för att välja rätt säkerhetslösning.

Den verkliga kostnaden för säkerhet

Att välja antivirusskydd är inte längre en prisfråga om det vore så skulle alla företag vara skyddade genom gratis antivirusprogram. Det är inte heller en fråga om att välja den ledande aktören på marknaden. De styrkor som har fört fram en leverantör till en ledande position på marknaden är inte nödvändigtvis de egenskaper som skyddar dig idag, eller imorgon när din miljö förändras. Ändå väljer IT-avdelningar alltför ofta den leverantör som kan ge det bästa priset - eller ännu värre - de förnyar helt enkelt sin nuvarande lösning utan att utvärdera kostnader och effektivitet. Det behövs ett nytt sätt att utvärdera antivirusskydd. Vid Kaspersky Lab kallar vi det för Den verkliga kostnaden för säkerhet.

Undvika”IO:n som medför 1 000 utgifter”:

Den verkliga kostnaden för säkerhet är summan av alla kostnader som hör samman med användningen av ett antivirusskydd - allt det som måste kostnadsberäknas för att du verkligen ska förstå vad du betalar för skyddet av ditt nätverk och dina användare. Den verkliga kostnaden för säkerhet består av följande element:

- Skydd
- Prestationer
- Administration
- Support
- Pris

Om någon av dessa kostnadsdelar skenar iväg stiger den verkliga kostnaden. Slutsatsen kan bli att driftskostnaden för din antiviruslösning är mycket högre än inköpspriset.

Låt oss titta närmare på de fem faktorer som utgör Den verkliga kostnaden för säkerhet:

Skydd

Hur effektivt skyddar din lösning mot skadlig programvara? Arbetar företaget förutseende med metoder för att skydda ny teknik (t.ex. moln, virtuella datorer osv.)?

Det primära målet för alla antiviruslösningar måste vara att skydda din IT-miljö mot virus, maskar, trojaner, spionprogram osv. Den första fråga du bör ställa dig när du utvärderar ditt antivirusprogram är, fungerar det och gör det vad det är tänkt att göra?

Ett dåligt eller otillräckligt skydd kan orsakas av:

- Sporadiska uppdateringar, så att systemet lämnas oskyddat för nya hot
- Falska varningar som stjäler dyrbara IT-resurser
- Felaktiga uppdateringar som stänger ned systemet
- Misslyckande i att detektera och förhindra skadlig programvara från att infektera systemet
- Misslyckande i att rensa upp och ta bort virus som har infekterat systemet, vilket kräver manuella lösningar
- Oförmåga att skydda heterogena nätverk och/eller nya tekniker, vilket kräver användning av flera olika lösningar

Ett antivirusprogram som inte ger tillräckligt skydd av någon av ovanstående orsaker kan öka dina kostnader rejält i form av dataförluster, minskad produktivitet hos dina anställda, utnyttjande av IT-resurser för systemåterställning, ekonomiska förluster som en följd av cyberbrottslighet och skadat renommé för ditt företag.

Prestanda

Offrar du prestanda för skydd?

Priset för skyddet får inte påverka slutanvändarnas produktivitet eller effektiviteten på arbetsplatsen. Trots allt är skyddet inte mycket värt om det hindrar slutanvändarna från att göra sitt jobb. Bloatware som det ofta kallas använder så mycket systemresurser att användarna inte kan använda sitt datorsystem förrän skanningen är klar. Tänk dig att varje slutanvändare tar en ”kafferast” på 30 minuter varje gång som systemet skannas eller virussignaturer uppdateras. Inga funktioner som systemskanning, nedladdning av signaturuppdateringar och uppgraderingar till nya versioner av leverantörens program får påverka den anställdes produktivitet eller effektiviteten på arbetsplatsen. När det gör det ökar Den verkliga kostnaden för säkerhet dramatiskt.

Administration

Hur mycket personal behövs för att hantera din säkerhetslösning och hur mycket arbetstid behövs för jobbet?

Den administrativa konsolen är en viktig del i köpbeslutet om det är svårt att hantera säkerheten på grund av en klumpig, svårförståelig, resursintensiv administration kommer verksamheten att lida genom ökade kostnader för skyddet. Förutom de extra arbetstimmar som behövs för att hantera lösningen riskerar du luckor i skyddet som ett resultat av inkonsekventa regler eller den mänskliga faktorn. Även kostnaderna för personalutbildning kommer att öka. Administration ska vara enkel och lättarbetad men ändå granulär och kraftfull nog för att minska riskerna i din miljö. Rapporter ska ge översikt och ge förståelse för din syn på säkerhet.

Support

Vad kostar egentligen supporten?

Kostnaden för support är en av de minst uppmärksammade punkterna i ekvationen för Den verkliga kostnaden för säkerhet - men det kan ändå vara den mest smärtsamma. Många leverantörer kräver extra avgifter för support oavsett om du väljer standard eller premium och dessa avgifter måste inkluderas i Den verkliga kostnaden för säkerhet. Men det är bara början. Dålig support kan orsaka kostnader i form av långa stillestånd, en lång väntan på problemets lösning och härmed sammanhängande produktivitetsförsämringar.

Support är en kritisk komponent för företagets utveckling. I en studie nyligen från Deloitte sa IT-ansvariga att de var oroliga för säkerheten eftersom de insåg att deras egen personal inte hade den kunskap som behövdes.(3) Det innebär att leverantören av antivirusskyddet måste besitta denna expertkunskap - och kunna tillhandahålla den när det behövs.

Pris

Hur konkurrenskraftigt är priset?

Konkurrenterna i säkerhetsbranschen ägnar sig åt en extremt aggressiv prissättning. Även om inköpspriset definitivt är viktigt bör det knappast vara din första prioritet. De dyraste programmen är nödvändigtvis inte de bästa, och med de billigaste kan ”omkostnaderna” skjuta i höjden. Som vi har visat kan ett val av säkerhetslösning som enbart, eller i första hand, baseras på inköpspriset leda till att Den verkliga kostnaden för säkerhet blir hög.

Många företag betalar ett mycket högre pris än de tror för säkerheten och i många fall får de inte heller det skydd de behöver.

Den verkliga kostnaden för säkerheten enligt Kaspersky Lab

Alltsedan starten 1997 har Kaspersky Lab varit knivskarpt fokuserat på en enda sak: att skydda sina kunder mot hot från skadliga program. Under den här perioden har många av våra konkurrenter anammat ett bredare fokus och i många fall inneburit att deras förmåga att tillhandahålla ett förstklassigt antivirusskydd försämrats. Kaspersky Labs engagerade och förstklassiga team med över 800 antivirusforskare och antivirusingenjörer och mer än 2 000 anställda över hela världen håller outtröttligt siktet inställt på hot från skadlig programvara. Vårt mål är att vara bäst i vart och ett av de delmoment som tillsammans utgör Den verkliga kostnaden för säkerhet. Vi levererar:

- Förstklassig detektering av skadliga program

I oberoende tester av detektering av skadliga program placeras Kaspersky överst på listan bland alla viktiga antivirusleverantörer, inklusive Symantec, McAfee och CA.(4) I genomsnitt tar det endast en och en halv timme för Kaspersky att skriva och sprida en signaturfil för ett nytt virus, jämfört med två till fyra timmar för övriga leverantörer. Uppdateringar levereras till kunderna en gång i timmen för att de alltid ska ha det senast tillgängliga skyddet vilket minskar tidsrymden som du är sårbar. Risken att bli infekterad minskar och Den verkliga kostnaden för säkerhet minskar.

Stanley Mierzwa, ansvarig för IT-teknik vid The Population Council, berättar om sina erfarenheter av säkerhetsprogram och Kaspersky:

”Vi insåg omedelbart att Kasperskys program gör skillnad. Det blev färre angrepp och det hade en mycket positiv inverkan på verksamheten. Vi fick en markant effektivitetsökning.”

- Överlägsen funktion

Kaspersky tillhandahåller kontinuerligt bästa funktionalitet för att säkerställa slutanvändarnas produktivitet och skydd. Våra små och täta uppdateringar är effektivare och kräver inte dyrbar bandbredd, något som är särskilt viktigt för de fjärranslutningar som har mobila Internetuppkopplingar. Dessutom används minimalt med systemresurser.

Vid Great Batch Inc. märkte deras säkerhet- och Oracle-analytiker Mike Ciura omedelbart skillnaden med Kasperskys program:

”De som använder CAD och systemintensiva produkter upplevde inga som helst problem. Jag fick många uppskattande kommentarer om att det var snabbare och arbetade i bakgrunden utan att störa dem.”

• Enkel administration

Alla Kasperskys produkter hanteras centralt i en enda administrativ konsol. Tidsåtgången och resurserna som företaget behöver för att hantera till och med de största och mest komplexa IT-miljöer hålls härmed på en låg nivå. Den enkla och intuitiva konsolen har kraft att identifiera och hantera risker tvärs över hela företaget inklusive fjärranslutningar och mobila enheter. Det reducerar dramatiskt Den verkliga kostnaden för säkerhet.

George Thornton, ansvarig för nätverksdriften vid Montgomery Independent School District, uttalar sig om de inbesparade ”omkostnader” som Kaspersky Lab står för:

”Med vår tidigare leverantör krävdes flera konsoler. Med Kaspersky räcker det med en enda administrativ konsol. Den är smidigt automatiserad. Administrationen av vår AV-lösning krävde en arbetstid på en till två dagar i veckan. Nu handlar det om minuter per vecka.”

• Förstklassig support

Kasperskys standardsupport är gratis och har den kortaste väntetiden i branschen: mindre än fem minuter. Uppklarningsprocenten vid första samtalet är över 90 %, så dina problem blir snabbt lösta med minimal påverkan på dina IT-resurser. Vi minskar Den verkliga kostnaden för säkerhet genom att tillhandahålla lokal, snabb och effektiv support i standardpaketet och utan extra kostnader.

Terry Meitz, nätverksingenjör vid Peachtree Financial, säger så här om kvaliteten på Kasperskys support:

“Kasperskys support är helt fenomenal. Väntetiden är mycket kort. Supportteamet är mycket kompetent och fantastiska att samarbeta med. De löste inte bara problemet som var den direkta anledningen till kontakten utan vi fick dessutom lösningen på ett annat problem som vi råkade ut för under samtalet.”

• Konkurrenskraftigt pris

Kasperskys prisbild är konkurrenskraftig i förhållande till andra leverantörer av antivirusskydd och priset ligger ofta på samma nivå eller lägre än hos konkurrenterna. Våra kunder får ett bättre skydd till en lägre kostnad.

Vid Centre for Education & Training har systemadministratören Victor Andreev upptäckt Den verkliga kostnaden för säkerhet enligt Kasperskys definition:

”Kasperskys offert hamnade en bra bit under den dyra offerten från vår nuvarande leverantör. Med de fördelar som vi såg, tillsammans med det låga priset, behövdes ingen längre betänketid för att byta leverantör.”

Slutsats

Kaspersky Lab strävar efter att tillhandahålla den bästa verkliga kostnaden för säkerhet och det gäller inte enbart i dagsläget. Vår kärnverksamhet handlar om att förstå viktiga branschtrender, de möjligheter och risker som de utgör samt tillhandahålla lösningar som inte bara möter dagens hot utan även morgondagens. Vi planerar för framtiden genom att hela tiden förbättra prestanda och funktion hos vara produkter. Vi lägger hela tiden till nya funktioner för att skydda och hantera data. Vi bygger ut vår portfölj och investerar i teknik som skyddar kundernas föränderliga IT-miljö - för att kunna fortsätta att leverera den bästa verkliga kostnaden för säkerhet.

(1) Enligt Frost & Sullivans 2011 (ISC)2 Global Information Security Workforce Study sponsrad av (ISC)2 säger 74 % av de tillfrågade (proffs inom IT-säkerhet) runt om i världen att det behövs nya kunskaper för att hantera den molnbaserade datoranvändningen.

(2) 66 % av de tillfrågade i Frost & Sullivans studie rapporterade att deras budget för experttjänster inte ökat under 2011 och 63 % rapporterade att deras budget för outsourcing eller managed services står kvar på samma nivå.

(3) Deloitte 2010 Financial Services Global Security Study

(4) Länk till sidan på webbplatsen med oberoende testresultat

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

c4oa

KASPERSKY lab