
BEST PRACTICES -
ENCRYPTIE.
With Kaspersky, now you can.
kaspersky.nl/business
Be Ready for What's Next
KASPERSKY lab

INHOUD

ENCRYPTIE - ALLES DRAAIT OM DE DATA.

Proactieve gegevensbeveiliging is wereldwijd een must. In de meeste grote markten ter wereld is het nu voor organisaties van elke omvang nodig om initiatieven voor gegevensbeveiliging en privacy te implementeren. Van PCI-DSS tot HIPAA en SOX, van de Europese DPP tot de Japanse PIPA en de Britse wet op gegevensbescherming: de mondiale trend is dat autoriteiten van bedrijven eisen dat zij gevoelige informatie proactief beschermen. In Groot-Brittannië heeft toezichthouder ICO bijvoorbeeld gezegd dat gegevensverlies dat optreedt "waar geen gebruik is gemaakt van encryptie om de gegevens te beschermen" waarschijnlijk zal leiden tot regelgevende actie.

1. INLEIDING

In een recente enquête, uitgevoerd door Kaspersky Lab, gaf 29% van de bedrijven aan dat er mobiele apparaten zijn verloren of gestolen. Volgens Kensington wordt er elke 53 seconden een laptop gestolen.[1&2]

Als uw eerste reactie op de bovenstaande statistieken is te bedenken hoeveel het kost om de hardware te vervangen, richt u zich op het verkeerde probleem. Hardwarekosten kunnen belangrijk zijn voor uw organisatie, maar bij gegevensverlies zijn ze waarschijnlijk niet uw grootste zorg. Bij verlies of diefstal van een laptop of apparatuur gaat meer dan 80 procent van de kosten zitten in het repareren van het ontstane gegevenslek[3] , onafhankelijk van de bedrijfsomvang.

Tel daar het groeiend aantal overheidsboetes wegens gegevensinbreuk, de reputatieschade en het effect op de klantentrouw bij op en het is gemakkelijk in te zien hoe de kosten van gegevensinbreuk veel verder strekken dan het vervangen van hardware. Wereldwijd zegt 85 procent van de klanten over te stappen op een andere aanbieder als een bedrijf hun persoonlijke gegevens kwijt zou raken of gehackt zou worden; 47 procent zou gerechtelijke stappen nemen.[4]

En u hoeft een apparaat niet fysiek kwijt te raken om gevoelige gegevens te verliezen. Gevoelige bedrijfsinformatie, intellectueel eigendom en handelsgeheimen zijn hoofddoelen geworden van malwareaanvallen.

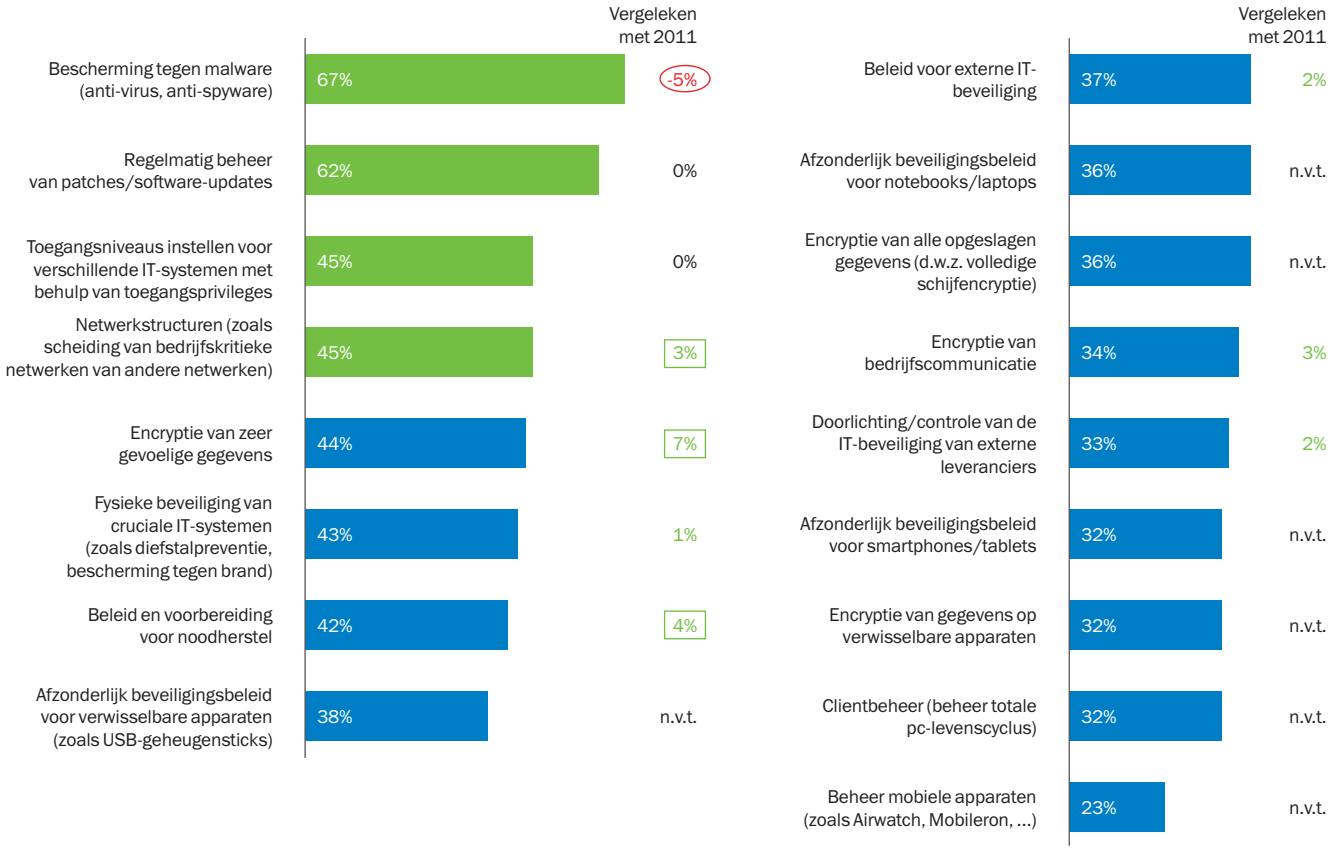
Volgens het Ponemon Institute bedraagt de gemiddelde waarde van een kwijtgeraakte laptop $ 49.246. Slechts 2 procent hiervan betreft de aanschafkosten van vervangende hardware. Encryptie kan de kosten van een laptop met gemiddeld meer dan $ 20.000 verlagen.[5] Of u nu te maken krijgt met een gestolen laptop, een zoekgeraakt opslagapparaat of malware die gegevens ontvreemdt, encryptie zorgt ervoor dat uw gevoelige informatie waardeloos is voor criminelen of onbevoegde lezers.

Hoe kunt u dit het beste aanpakken?

1 Bron: Kaspersky Global IT Risk Report 2012
2 Bron: Kensington: The Cost of Stolen or Lost Laptops, Tablets and Phones, 2012
3 Bron: Ponemon: The Billion Dollar Lost Laptop Problem (2012)
4 Bron: Unisys Security IndexTM: GLOBAL SUMMARY 18 oktober 2011 (Wave 2H'11)
5 Bron: Ponemon: The Cost of a Lost Laptop (2009)

2. BEST PRACTICES

Ooit werd encryptie gezien als iets dat was voorbehouden aan overheidsinstellingen of grote ondernemingen met nog ruimere budgetten. De technologie heeft echter niet stilgestaan. Tegenwoordig kunnen organisaties van elk formaat het zich permitteren om zuinige, gemakkelijk beheerbare encryptiesoplossingen te implementeren.



Encryptie is steeds vaker een wapen in de strijd tegen gegevensverlies.[6]

Op de volgende pagina's bespreken we enkele best practices die u kunt toepassen om ervoor te zorgen dat uw organisatie een effectieve encryptiesstrategie hanteert.

6 Bron: Kaspersky Global IT Risk Report 2012

3. EERST BELEID, DAN TECHNOLOGIE

Zoals geldt voor vele beveiligingsstrategieën, vormt het opstellen van een sterk beleid de basis voor de beste encryptiespraktijken: gaat u complete schijven coderen? Verwisselbare opslagapparaten? Of alleen bepaalde typen gegevens, bestanden en mappen? Wellicht wilt u dat bepaalde documenten onleesbaar zijn voor sommige gebruikers, maar niet voor anderen? Of misschien een beetje van beiden?

Voor de meeste bedrijven is het beschikbaar stellen van informatie aan de juiste mensen op het juiste moment een prioriteit – door goed beleid te koppelen aan de juiste technologieën kunt u dat bereiken zonder afbreuk te doen aan de beveiliging.

Enkele goede startpunten zijn:

- **Betrek alle relevante belanghebbenden** – IT-management, bedrijfsvoering, financiën. Zij zullen u helpen om het soort informatie te identificeren dat extra bescherming nodig heeft.
- **Toegangscontrole** – Als iedereen een sleutel heeft, is het zinloos om de deur op slot te doen. Identificeer samen met de belanghebbenden wie er toegang moet krijgen tot welk soort informatie. En wanneer. Controleer als extra voorzorgsmaatregel regelmatig de toegangsregeling, zodat deze relevant blijft.
- **Ken uw compliancebehoeften** – PCI-DSS, HIPAA, SOX, de Europese DPP, de Japanse PIPA of de Britse wet op gegevensbescherming. Wellicht bent u niet bekend met het groeiend aantal regels op het gebied van gegevensbeveiliging, maar veel van uw collega's zijn dat wel. Identificeer de regelgeving, wetten, richtlijnen en andere externe factoren die bepalen op welke manier gegevens worden beveiligd of uitgewisseld binnen de organisatie. Stel beleidslijnen vast om hierop in te spelen – bijvoorbeeld automatische encryptie van de creditcardgegevens van klanten of burgerservicenummers van personeel.
- **Er helemaal of helemaal niet voor gaan** – Zet uw beleid op papier, laat dit door het senior management onderschrijven en communiceer het naar uw eindgebruikers, inclusief derden die uw gevoelige gegevens hanteren. Mochten zij hier niet achter staan, dan krijgen ze geen toegang tot uw gegevens.
- **Maak een back-up** – Best practice is om altijd een back-up van uw gegevens te maken voordat u nieuwe software installeert. Dit geldt ook voor encryptie: zorg ervoor dat u een back-up maakt van alle gegevens van de eindgebruiker voordat u uw encryptiesprogramma erop loslaat.

4. ENCRYPTIE VAN DE HELE SCHIJF OF OP BESTANDSNIVEAU?

Het antwoord is eenvoudig: allebei. Standaard zijn er twee soorten encryptiesoplossingen – volledige schijfencryptie (Full Disk Encryption; FDE) en encryptie op bestandsniveau (File Level Encryption; FLE). Elk van beide heeft zijn eigen voordelen:

4.1 Voordelen van volledige schijfencryptie (FDE):

- FDE beschermt opgeslagen gegevens op het niveau dat zo dicht mogelijk bij de hardware ligt – dat wil zeggen dat elke afzonderlijke sector op de schijf wordt gecodeerd. Dit betekent dat alle gegevens op uw harde schijf zijn gecodeerd, inclusief de inhoud van bestanden, metagegevens, bestandssysteeminformatie en mappenstructuur. Alleen geverifieerde gebruikers kunnen toegang krijgen tot gegevens op de gecodeerde schijf. FDE-technologie kan niet alleen worden toegepast op harde schijven, maar ook op verwisselbare media zoals USB-schijven of harde schijven in apparatuur die op de USB-poort kan worden aangesloten.
- Zorg voor 'pre-boot'-verificatie – hierbij moet de gebruiker met succes een verificatieproces doorlopen voordat het besturingssysteem überhaupt wordt opgestart. Dit biedt u een extra beveiligingslaag als uw laptop kwijt is of is gestolen – dieven kunnen niets direct vanaf de schijf lezen, noch kan het besturingssysteem worden gestart.
- Best practice voor FDE omvat ook een zogenoemd 'set and forget'-beleid, waardoor de eindgebruiker geen rol meer speelt; zorg voor toegang via eenmalig inloggen (single sign-on; SSO) en uw eindgebruikers hoeven verder niks te weten.
- Het grootste voordeel van FDE is dat het gebruikersfouten als risicobron elimineert – het codeert simpelweg alles. Het nadeel is dat het geen gegevens kan beschermen tijdens de overdracht ervan, waaronder informatie die wordt gedeeld door meerdere apparaten. Houdt u zich aan de best practices en kiest u voor een oplossing die ook encryptie op bestandsniveau biedt, dan is dit voor u geen probleem.

4.2 Voordelen van encryptie op bestandsniveau (FLE):

FLE werkt op het niveau van het bestandssysteem en biedt niet alleen bescherming van opgeslagen gegevens, maar ook beveiliging van gegevens die in gebruik zijn. Met behulp van FLE kunnen specifieke bestanden en mappen op elk willekeurig apparaat worden gecodeerd. Hoogwaardige oplossingen zorgen ervoor dat gecodeerde bestanden gecodeerd blijven, zelfs als ze binnen het netwerk worden gekopieerd. Hierdoor is de geselecteerde informatie onleesbaar voor ongeautoriseerde personen, of deze nu is opgeslagen of wordt gekopieerd. FLE stelt beheerders in staat om automatisch bestanden te coderen op basis van eigenschappen zoals locatie (bijvoorbeeld alle bestanden in de map Mijn Documenten), bestandstype (bijvoorbeeld alle tekstbestanden, alle Excel-spreadsheets enz.) of de naam van de applicatie die het bestand heeft geschreven – een hoogwaardige oplossing zal bijvoorbeeld de encryptie ondersteunen van gegevens die zijn geschreven door Microsoft Word, in welke map of op welke schijf ze zich ook bevinden.

- FLE biedt een hoge mate van flexibiliteit aan bedrijven die een nauwkeurig informatietoegangsbeleid willen toepassen – alleen gegevens die als gevoelig zijn gedefinieerd (volgens de door de beheerder opgestelde richtlijnen) worden gecodeerd, wat gemengd gegevensgebruik mogelijk maakt.
- FLE maakt ook eenvoudig en veilig systeemonderhoud mogelijk – gecodeerde bestandsgegevens kunnen beveiligd blijven terwijl software of systeembestanden worden gebruikt om updates of ander onderhoud uit te voeren. Als u bijvoorbeeld een CFO bent die vertrouwelijke bedrijfsinformatie niet onder ogen van een systeembeheerder wil laten komen, dan wordt dit door FLE ondersteund.
- FLE ondersteunt effectieve autorisatiecontrole van toepassingen, waardoor beheerders duidelijke encryptiesregels kunnen configureren voor specifieke applicaties en gebruiksscenario's. Door middel van autorisatiecontrole van toepassingen besluiten beheerders wanneer gecodeerde gegevens in hun gecodeerde vorm worden aangeboden of de toegang tot gecodeerde gegevens voor bepaalde applicaties zelfs helemaal wordt geblokkeerd, zoals:
  - Veilige back-ups vereenvoudigen door te verzekeren dat gecodeerde gegevens tijdens overdracht, opslag en herstel gecodeerd blijven, onafhankelijk van de beleidsinstellingen op het endpoint waar de gegevens worden hersteld.
  - Uitwisseling van gecodeerde bestanden via IM voorkomen, zonder legitieme berichtuitwisseling te beperken.

Door voor een gecombineerde FDE/FLE-aanpak van encryptie te kiezen, kunnen bedrijven profiteren van de voordelen van beide encryptieen – u kunt bijvoorbeeld voor bestandsencryptie kiezen op desktop-pc's en voor volledige schijfencryptie op alle laptops.

5. ZORG VOOR Encryptie VAN VERWISSELBARE MEDIA

USB-flashdrives kunnen tegenwoordig meer dan 100 GB aan gegevens bevatten, terwijl draagbare schijven die in de palm van uw hand passen, plaats bieden aan terabytes aan gegevens – heel wat mogelijk bedrijfsgevoelige informatie kan zo achterblijven in jaszakken bij de stomerij, bij de veiligheidscontrole op de luchthaven of simpelweg uit uw zak vallen.

U hebt onzorgvuldige gebruikers of ongelukken niet in de hand, maar de gevolgen daarvan wel. Apparaatencryptie is standaard onderdeel van effectieve encryptiesstrategieën. Zorg ervoor dat gevoelige gegevens altijd gecodeerd zijn als zij worden overgedragen van een endpoint naar een verwisselbaar apparaat. Dit kunt u bereiken door het FDE- of FLE-beleid toe te passen op alle apparaten. Zo verzekert u dat uw gevoelige gegevens zelfs bij verlies of diefstal van deze apparatuur beveiligd zijn.

Zowel binnen als buiten de perimeter moet bij het werken met gevoelige informatie de zogenoemde 'draagbare modus' worden gebruikt. Stel, u geeft een presentatie op een conferentie en moet een flashdrive gebruiken om uw gegevens over te zetten op een openbare computer waarop geen encryptiessoftware is geïnstalleerd. Dan moet u ervoor zorgen dat uw gegevens beveiligd blijven, zelfs gedurende de overdracht van uw laptop naar het presentatiesysteem – hoogwaardige oplossingen bieden een 'draagbare modus' waarmee u dit kunt bereiken. Deze zorgt voor transparant gebruik en overdracht van gegevens op gecodeerde verwisselbare media, zelfs naar computers waarop geen encryptiessoftware is geïnstalleerd.

6. KIES VOOR BEWEZEN VEILIGE CRYPTOGRAFIE

Hoe goed uw encryptiesstrategie ook is, als de onderliggende technologie niet goed is, hebt u er weinig aan. Eenvoudig te breken encryptiesalgoritmen zijn waardeloos. Advanced Encryption Standard (AES) met een 256-bits sleutel wordt gezien als de 'gouden standaard' van versleutelingstechnieken. Deze wordt gebruikt door de Amerikaanse overheid en is wereldwijd de norm voor de sector. Onderschat het belang van sleutels niet – uw encryptiesalgoritme is slechts zo goed als de sleutel die nodig is om hem te ontcijferen. Als de sleutels eenvoudig zijn te hacken, is uw volledige encryptiesprogramma nutteloos. Zo is effectief sleutelbeheer ook een essentieel onderdeel van effectieve encryptie – het heeft geen zin om het beste slot ter wereld op uw deur te hebben als u de sleutel onder de deurmat legt.

7. VERGEET U NIET TEGEN MALWARE TE BESCHERMEN

Zelfs bij laptops die niet zijn kwijtgeraakt of gestolen, bestaat er nog steeds risico op gegevensverlies. Steeds vaker kiezen cybercriminelen gevoelige informatie op bedrijfsapparatuur als doelwit en schrijven ze schadelijke codes die gegevens uit een laptop kunnen stelen zonder dat de gebruiker het weet.

Geen enkele best practice-strategie op het gebied van encryptie is compleet zonder geïntegreerde anti-malware die in staat is om schadelijke codes aan te pakken die erop gericht zijn om waardevolle informatie vanuit uw laptop te stelen. Best practice vraagt om anti-malware-updates en scancapaciteiten die automatisch kunnen worden uitgevoerd, zonder tussenkomst van de eindgebruiker.

8. WACHTWOORD VERGETEN

Gebruikers vergeten bijna net zo vaak hun wachtwoord als dat ze hun USB-sticks of smartphones verliezen. Soms kan zelfs de beste hardware of het beste besturingssysteem het laten afweten, waardoor gebruikers geen toegang hebben tot essentiële informatie. Bewaar encryptiessleutels op een centrale opslaglocatie of bij een derde partij (escrow) – dit maakt het een stuk makkelijker voor u om gegevens te decoderen in noodsituaties.

Een goede encryptiesoplossing moet beheerders voorzien van tools waarmee gegevens op een gemakkelijke manier zijn te herstellen in de volgende gevallen:

- Wanneer de eindgebruiker hieraan behoefte heeft (bijvoorbeeld als hij zijn wachtwoord heeft vergeten)
- Wanneer de beheerder dit nodig heeft voor onderhoud of bij technische problemen, zoals een besturingssysteem dat niet kan worden geladen of een harde schijf die fysieke schade heeft opgelopen en moet worden gerepareerd.

Wanneer gebruikers hun wachtwoord vergeten, is alternatieve verificatie mogelijk door van hen het juiste antwoord te verlangen op een serie alternatieve vragen.

9. HOUD HET SIMPEL, HOUD HET CENTRAAL

Van oudsher is een vaak gehoorde klacht van bedrijven die encryptie willen toepassen dat de implementatie en het beheer ervan te ingewikkeld zijn. Veel oudere oplossingen omvatten geen anti-malware, wat voor een extra complexiteitslaag zorgt. Zelfs als ze van dezelfde leverancier afkomstig zijn (om niet te spreken van omgevingen met programma's van meerdere leveranciers!), is het beheren van meerdere oplossingen - anti-malware, endpointbeheer, encryptie - niet alleen duur maar ook tijdrovend gedurende alle implementatie- en gebruiksfasen: aanschaf, training van personeel, provisioning, beleidsbeheer, onderhoud en upgrade moeten voor elke component als afzonderlijk project worden behandeld. Een geïntegreerde aanpak bespaart niet alleen tijd en geld, maar maakt ook het implementatieproces van de software zo gemakkelijk en moeiteloos mogelijk.

Eenvoudig te beheren oplossingen zijn effectiever. Kies er een die vanaf de eerste dag het gebruik van een enkele console en een enkel beleidsbeheer mogelijk maakt. Dan hoeft u minder te investeren en elimineert u compatibiliteitsproblemen tussen talrijke componenten die elk afzonderlijk moeten worden beheerd. De aanbevolen werkwijze is om encryptiesinstellingen op het endpoint onder hetzelfde beleid toe te passen als anti-malware, apparaatbeheer en alle andere beveiligingsinstellingen op het endpoint. Hierdoor is de best practice-aanpak mogelijk van een geïntegreerd, samenhangend beleid – de IT-afdeling kan bijvoorbeeld niet alleen goedgekeurde verwisselbare media toestaan om verbinding te maken met een laptop, maar kan het apparaat ook encryptiesbeleid opleggen. Een aanvullend voordeel van een goed geïntegreerd technologieplatform is dat het de totaalprestaties van het systeem verbetert.

10. SAMENVATTING

Kaspersky Endpoint Security for Business kan ondernemingen van elke omvang helpen om best practices op het gebied van encryptie een realiteit te maken. Ons geïntegreerde platform combineert encryptietechnologie op het hoogste niveau met Kaspersky's toonaangevende technologieën voor anti-malware en endpointbeheer. Zo helpt het gevoelige gegevens te beschermen tegen de risico's die verbonden zijn aan verlies of diefstal van apparatuur en voorkomt het de ontvreemding van informatie door malware.

Nauwkeurig beheer en rijke functionaliteit zijn eenvoudig in te zetten vanuit één enkele, centrale beheerconsole. Dit biedt beheerders echt één overzicht over hun beveiligingslandschap – of het nu gaat om virtuele machines, fysieke of mobiele/verwisselbare apparaten.

In tegenstelling tot vele traditionele gegevensbeveiligingsoplossingen maakt Kaspersky Endpoint Security for Business enkelvoudig beleidsbeheer vanaf de basis mogelijk: encryptiebeleid wordt ingesteld binnen hetzelfde totaalbeleid dat geldt voor anti-malware, apparaatbeheer, applicatiebeheer en alle andere beveiligingsinstellingen op het endpoint. Deze aanpak vanaf de basis is mogelijk dankzij Kaspersky's uniforme basiscode – onze ontwikkelaars creëren software en technologieën die naadloos communiceren, waardoor gebruikers beschikken over een beveiligingsplatform in plaats van een onsamenhangende suite.

Nauwe integratie van essentiële beveiligingsonderdelen zoals anti-malware, encryptie, applicatie- en apparaatbeheer maakt beheer en bewaking eenvoudiger, terwijl stabiliteit, geïntegreerd beleid, rapportages en intuïtieve tools worden geleverd.

ÉÉN CONSOLE. ÉÉN PLATFORM. ÉÉN PRIJS.

SEE IT. CONTROL IT. PROTECT IT.

With Kaspersky, now you can.
kaspersky.nl/business

Be Ready for What's Next

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