KASPERSKY lab

BEST PRACTICES

Encryptie

kaspersky.com/nl

ENCRYPTIE - BEST PRACTICES

Gegevensbeveiliging. Kom in actie.

Proactieve gegevensbeveiliging is een must voor bedrijven over de hele wereld. Kaspersky Lab kan u helpen om best practices voor gegevensencryptie en -beveiliging te implementeren.

Het zakelijke belang van encryptie

Sinds 2005 zijn meer dan **816** miljoen gegevensrecords ten prooi gevallen aan kwaadwillenden.[1] Alleen al gedurende de eerste vier maanden van 2015 werden **101** miljoen records ontmaskerd.[2]

Er gaat haast geen week voorbij of je hoort wel weer een nieuwsbericht over een inbreuk op de gegevensbeveiliging bij een organisatie. Het Identity Theft Resource Center kenschetste 2014 als 'het jaar van de gegevensinbreuk'. Volgens deze organisatie zijn de opslag van gegevens op mobiele of verwisselbare apparaten en interne gegevensinbreuken door onbevoegde medewerkers de twee belangrijkste oorzaken van het verlies of lekken van vertrouwelijke informatie.[3] Uit een enquête van Kaspersky Lab bleek dat bijna één op de vijf bedrijven wel eens gegevensverlies had geleden als direct gevolg van diefstal van een apparaat.[4]

Kaspersky Lab becijferde dat in 2014 de gemiddelde kosten van gegevensverlies per incident voor grote ondernemingen **EUR 568.000** en voor MKB-bedrijven **EUR 29.500** bedroegen.[5] 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.

Maar het gaat niet alleen om de directe kosten van een inbreuk, het verlies van trouwe klanten of reputatieschade voor uw bedrijf (72 procent van de geënquêteerde bedrijven moest publiekelijk erkennen te zijn getroffen door een incident[6]); in de meeste grote markten zijn gegevensbeveiliging en privacy inmiddels bij wet voorgeschreven, terwijl in veel rechtsgebieden organisaties verplicht zijn om vertrouwelijke gegevens van encryptie te voorzien.

Of het nu PCI-DSS, HIPAA, SOX, de Europese DPP, de Japanse PIPA of de Britse wet op gegevensbescherming betreft: 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 codering om de gegevens te beschermen” waarschijnlijk zal leiden tot regelgevende actie.

Of u nu te maken krijgt met een gestolen laptop, een zoekgeraakt opslagapparaat of malware die gegevens ontvreemdt, codering zorgt ervoor dat uw gevoelige informatie waardeloos is voor criminelen of onbevoegde lezers.

Hoe kunt u dit het beste aanpakken?

1 Privacy Rights Clearing House: http://www.privacyrights.org/data-breach
2 Identity Theft Resource Center 2015: http://www.idtheftcenter.org/images/breach/ITRCBreachStatsReport2015.pdf
3 Identity Theft Resource Center 2015: http://www.idtheftcenter.org/Press-Releases/2014breachstatistics.ht
4 Kaspersky Lab: 2014 IT Security Risks Report
5 Kaspersky Lab: 2014 IT Security Risks Report
6 Kaspersky Lab: 2014 IT Security Risks Report

Best practices voor encryptie

De encryptietechnologie van Kaspersky Lab beschermt waardevolle gegevens bij verlies of diefstal van apparaten en gerichte malwareaanvallen.

1. EERST BELEID, DAN TECHNOLOGIE

Net als bij veel andere beveiligingsstrategieën begint ook de best practice voor encryptie met het opstellen van krachtige beleidsregels: Gaat u hele schijven van encryptie voorzien? 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 beide?

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 belanghebbende partijen** – IT-beheer, Operations, Finance, HR, enzovoort. Zij helpen u bepalen welke soorten informatie extra beveiliging nodig hebben.
- **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.
- **Weet aan welke wetgeving u zich dient te houden** – 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 codering 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** – Een goede best practice is om altijd een back-up van uw gegevens te maken voordat u nieuwe software installeert. Dit geldt ook voor codering: zorg ervoor dat u een back-up maakt van alle gegevens van de eindgebruiker voordat u uw coderingsprogramma erop loslaat.
- **Houd het simpel** – minimaliseer de belasting voor eindgebruikers door technologie te implementeren die eenmalig inloggen (single sign-on; SSO) ondersteunt.

2. ENCRYPTIE VAN DE HELE SCHIJF OF OP BESTANDSNIVEAU?

Het antwoord is eenvoudig: allebei.

Standaard zijn er twee soorten coderingsoplossingen – volledige schijfcodering (Full Disk Encryption; FDE) en codering op bestandsniveau (File Level Encryption; FLE). Elk van beide heeft zijn eigen voordelen:

Voordelen van volledige schijfcodering (FDE):

FDE is een van de meest effectieve manieren waarop een organisatie haar gegevens kan beschermen tegen diefstal of verlies. Met FDE kunnen organisaties garanderen dat alle gevoelige gegevens geheel onleesbaar en dus nutteloos zijn voor criminelen of nieuwsgierige ogen, wat er ook met het apparaat gebeurt.

- FDE beschermt opgeslagen gegevens op een niveau dat zo dicht mogelijk bij de hardware ligt – dat wil zeggen dat elke afzonderlijke sector op de schijf van encryptie wordt voorzien. 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.

- Profiteer van Pre-Boot Authentication (PBA) – PBA vereist dat gebruikers hun inloggegevens invoeren en laten controleren nog voordat het besturingssysteem opstart, wat een extra beveiligingslaag toevoegt. Kwaadwillenden kunnen geen gegevens rechtstreeks uitlezen van het oppervlak van de harde schijf en ook het besturingssysteem kan niet worden gestart.

  De encryptietechnologie van Kaspersky Lab voorziet niet alleen in PBA met optionele single sign-on (SSO), maar biedt ook andere toetsenbordindelingen dan QWERTY voor een betere gebruikerservaring. Encryptieoplossingen met ondersteuning voor dubbele verificatie via smartcards en tokens maken extra wachtwoorden overbodig, wat de gebruikerservaring eveneens ten goede komt.

- Profiteer van een encryptieoplossing die **vóór** de implementatie controleert op compatibiliteit met alle netwerkhardware, zodat u achteraf geen kopzorgen hebt. Oplossingen die ondersteuning bieden voor UEFI-gebaseerde platforms, waaronder de nieuwste laptops en werkstations met Windows 8 of later, zorgen dat u klaar bent voor de toekomst.

  Bovendien dragen ondersteuning voor Intel® AES NI – een nieuwe verbetering van de Advanced Encryption Standard (AES) die encryptie versnelt voor Intel®s Xeon- en Core-processors (evenals sommige AMD-processors) – en de nieuwste GPT-schijfstandaarden bij aan een complete encryptiestrategie.

- Maak veilig delen van gegevens binnen het bedrijf mogelijk door FDE-encryptie te gebruiken voor verwisselbare stations.

- 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. Dubbele verificatie voorziet in een extra beveiligingslaag en maakt extra gebruikersnamen en wachtwoorden overbodig, wat de gebruiksvriendelijkheid verder verhoogt. Encryptieoplossingen die Role-Based Access Control (RBAC) ondersteunen, maken het delegeren van beheer op basis van rol/functie mogelijk, waardoor het encryptiebeheer minder complex wordt.

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 codering op bestandsniveau biedt, dan is dit voor u geen probleem.

Voordelen van codering op bestandsniveau (FLE):

Doordat FLE op het niveau van het bestandssysteem werkt, worden niet alleen de 'gegevens in rust' beveiligd, maar ook de 'gegevens in gebruik'. Met FLE kunnen specifieke bestanden en mappen op welk apparaat dan ook van encryptie worden voorzien. 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 toepassing die het bestand heeft geschreven – een hoogwaardige oplossing zal bijvoorbeeld de codering 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 van encryptie voorzien, 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 coderingsregels kunnen configureren voor specifieke toepassingen en gebruiksscenario's. Door middel van autorisatiecontrole van applicaties 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 codering te kiezen, kunnen bedrijven profiteren van de voordelen van beide coderingen – u kunt bijvoorbeeld voor bestandscodering kiezen op desktop-PC's en voor volledige schijfcodering op alle laptops.

3. 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.

Apparaatcodering is standaard onderdeel van effectieve coderingsstrategieën. 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.

De meest effectieve encryptieoplossingen integreren met uitgebreide apparaatbeheermogelijkheden om een nauwkeurige toepassing van beleidsregels mogelijk te maken, bijvoorbeeld voor specifieke apparaatserienummers.

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 coderingssoftware 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 coderingssoftware is geïnstalleerd.

Kies voor bewezen veilige cryptografie

Hoe goed uw coderingsstrategie ook is, als de onderliggende technologie niet goed is, hebt u er weinig aan. Eenvoudig te breken coderingsalgoritmen zijn waardeloos. Kies een encryptieoplossing die Advanced Encryption Standard (AES) gebruikt met een sleutellengte van 256 bits, met vereenvoudigd sleutelbeheer en opslag bij derden. Met ondersteuning voor Intel® AES-NI-technologie, UEFI en GPT-platforms bent u er zeker van dat uw strategie toekomstbestendig is.

Onderschat het belang van sleutels niet – uw coderingsalgoritme is slechts zo goed als de sleutel die nodig is om hem te ontcijferen. Als de sleutels eenvoudig zijn te hacken, is uw volledige coderingsprogramma nutteloos. Zo is effectief sleutelbeheer ook een essentieel onderdeel van effectieve codering – het heeft geen zin om het beste slot ter wereld op uw deur te hebben als u de sleutel onder de deurmat legt.

Kies voor meerlaagse beveiliging

Eindgebruikers en verloren apparaten zijn niet de enige oorzaken van gegevensverlies. Gegevensdieven ontwikkelen steeds geavanceerdere malware om systemen binnen te dringen en gegevens te stelen. Dit soort incidenten blijft vaak jarenlang onopgemerkt. Hoewel encryptie helpt om gestolen gegevens onbruikbaar te maken, is het is veel effectiever om encryptie als een complementaire laag van een bredere, geïntegreerde beveiligingsstrategie te zien, waarin kwalitatief hoogwaardige anti-malware, apparaat- en applicatiebeschermingsmechanismen samenwerken om de kans te verkleinen dat cybercriminelen zichzelf toegang verschaffen tot uw systemen en uw vertrouwelijke gegevens stelen.

Geen enkele encryptiestrategie is compleet zonder geïntegreerde lagen van anti-malware en op controlemechanismen gebaseerde beveiliging die in staat is om schadelijke code te detecteren en uit te schakelen, en zwakke plekken die organisaties blootstellen aan gegevensverlies, te identificeren en te beheren. Dit dient allemaal te gebeuren met een minimale verstoring van eindgebruikers, of liever nog onopgemerkt.

Uw 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 coderingssleutels 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 coderingsoplossing 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 bij 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.

Centraal beheren

Encryptie heeft de naam gekregen te lastig te implementeren en beheren te zijn. Dat komt vooral doordat traditionele, gedateerde oplossingen werden geleverd die niet samenwerkten met anti-malware en andere IT-beveiligingstechnologieën, waardoor de implementatie en het beheer onnodig complex werden. Zelfs als ze van dezelfde leverancier afkomstig zijn, 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 volledig geïntegreerde, meerlaagse beveiligingsoplossing 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 één enkele console en één 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 coderingsinstellingen 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 coderingsbeleid opleggen. Een aanvullend voordeel van een goe geïntegreerd technologieplatform is dat het de totaalprestaties van het systeem verbetert.

TOT SLOT...

Kaspersky Endpoint Security for Business kan ondernemingen van elke omvang helpen om best practices op het gebied van codering een realiteit te maken.

Volledige integratie met de hoogwaardige anti-malware, endpointbeheer en beheertechnologieën van Kaspersky Lab voor een meerlaagse beveiliging met een gemeenschappelijke codebasis. U kunt encryptie-instellingen op het endpoint toepassen onder hetzelfde beleid als anti-malware, apparaatbeheer en alle andere onderdelen voor endpointbeveiliging. Zo hebt u niet langer verschillende oplossingen nodig. De compatibiliteit van netwerkhardware wordt automatisch gecontroleerd voordat de encryptie wordt uitgevoerd en UEFI- en GPT-platformen worden standaard ondersteund.

Deze aanpak vanaf de basis is mogelijk dankzij de uniforme codebasis van Kaspersky. Onze ontwikkelaars creëren software en technologieën die naadloos communiceren, waardoor gebruikers beschikken over een geïntegreerd beveiligingsplatform in plaats van een onsamenhangende suite.

Eén leverancier, één prijs, één installatie, complete beveiliging.


Twitter.com/
Kaspersky


Facebook.com/
Kaspersky


Youtube.com/
Kaspersky

Kaspersky Lab
kaspersky.com/nl

Alles over internetbeveiliging:
www.securelist.com

Zoek een partner bij u in de buurt:
http://www.kaspersky.com/nl/partners

KASPERSKY lab