IDC EMEA, 389 Chiswick High Road, Londen, W4 4AE, Verenigd Koninkrijk Tel. +44.20.8987.7100 www.idc.com

WHITEPAPER

Laptopbeveiliging: de dreiging voor het MKB van verlies of diefstal van laptops

Sponsor: Kensington

Phil Odgers

Augustus 2007

Inleiding

Het vinden van de juiste instrumenten voor taken wordt steeds belangrijker voor het midden- en kleinbedrijf. In de concurrentie met grote bedrijven die schaalvoordeel hebben of echt kleine bedrijven die dynamisch zijn door hun flexibiliteit en die een lagere overhead hebben, moet het midden- en kleinbedrijf elk concurrentievoordeel uitbuiten.

Het is gemakkelijk te begrijpen waarom de laptop zo populair is in het midden- en kleinbedrijf: de productiviteit neemt toe, de klantenservice wordt beter en de reiskosten worden gedrukt. De voordelen zijn groot en de prijzen van hardware zijn de laatste tien jaar sterk gedaald.

Deze populariteit zorgt echter ook voor nieuwe uitdagingen voor bedrijven. Kostbare gegevens bevonden zich vroeger veilig achter de deuren van de serverruimte of op PC's op kantoor, maar nu lopen medewerkers buiten rond met hun gegevens op de laptop. De kostbare apparaten met hun waardevolle bedrijfsinformatie brengen de gelegenheidsdief in verleiding, om nog maar te zwijgen over de professionele dief. Hardware is echter niet het enige dat gevaar loopt...

Er zijn nog andere overwegingen voor het midden- en kleinbedrijf. De kosten voor de hardware na diefstal zijn nog wel op te vangen, maar de verstoring van de bedrijfsprocessen en het verlies van kostbare gegevens (klantgegevens, medewerkerinformatie of gevoelige bedrijfsinformatie) is veel erger. Verstoring van de bedrijfsprocessen is iets dat het midden- en kleinbedrijf vaak niet meeneemt in de overweging als diefstal van laptops wordt bekeken. De vervanging van gestolen hardware en de invloed op de continuïteit van relaties met klanten en van processen zijn vaak veel schadelijker. Dit IDC-document laat zien dat het echte probleem voor het midden- en kleinbedrijf het verlies van gegevens is en laat zien hoe volgens veel ICT-managers het aantal diefstallen sterk kan worden teruggebracht met enkele eenvoudige maatregelen.

Methodologie

Deze bevindingen zijn gebaseerd op de uitkomsten van 200 interviews met vertegenwoordigers van het midden- en kleinbedrijf in het Verenigd Koninkrijk, Frankrijk en de Benelux. De interviews werden gehouden in juni 2007. Alle respondenten waren ICT-managers of netwerkbeveiligingsspecialisten. Deze mensen waren verantwoordelijk voor de ICT-beslissingen in hun organisatie en met name het aanschaffen en vervangen van laptops, en de beveiliging van het netwerk van hun organisatie.

De geïnterviewde organisaties varieerden in grootte van 50 tot 500 medewerkers.

Alle bevindingen werden geanalyseerd in de context van bestaande inzichten van de IDC in de beveiliging van laptops. Waar relevant werden vergelijkingen getrokken en verschillen aangegeven met de gegevens van een Europees onderzoek naar de beveiliging en diefstal van laptops uit 2005.

In dit document

Dit document bespreekt de beveiliging van laptops, behandelt de bedreigingen van de diefstal van het apparaat zelf en kijkt naar manieren om de risico's te minimaliseren. Dit document legt de nadruk op het kweken van begrip bij leidinggevenden en beslissers voor de situatie zoals die nu is bij het midden- en kleinbedrijf. Ook wordt beschreven hoe ze hun bedrijf en bedrijfsbelangen kunnen beschermen tegen de diefstal van laptops.

Hoofddoel

Het minimaliseren van het risico van diefstal van laptops moet niet alleen de zorg van de ICT-manager zijn, maar van elke medewerker die een laptop tot zijn beschikking heeft. Eenvoudige maatregelen die het risico op diefstal verminderen moeten worden gecombineerd met een afweging van het risico op diefstal versus het voordeel van de beschikbaarheid van gegevens onderweg. Er moet worden afgewogen welk type gegevens een acceptabel risico vormen en welk type beter op een bedrijfsnetwerk kan worden opgeslagen.

De volgende maatregelen zijn eenvoudig en elke ICT-afdeling zou ze moeten nemen om de aantrekkelijkheid van hun mobiele hardware voor een dief te verminderen:

- Onopvallende tassen
- Controleer de apparatuur op labels of duidelijk in het oog springende naamstickers.
- Beleid dat laptops die onbewaakt worden achtergelaten altijd met een kettingslot moeten worden vastgemaakt.
- Beleid dat altijd een kettingslot wordt gebruikt op openbare plaatsen.

Wat gebeurt er als er een laptop wordt gestolen?

Het is bekend de kans dat een Europees midden- of kleinbedrijf een gestolen laptop terugkrijgt kleiner is dan 3%. Veel is niet bekend over de resterende 97%, maar het is wel bekend dat slechts een klein deel wordt gestolen vanwege de gegevens. Gerichte diefstal van de laptops van belangrijke medewerkers vindt plaats om de gegevens die ze bevatten te verkopen. Een vraag die u nooit beantwoord zult krijgen is *Hoe kan ik er zeker van zijn dat er niet meer gestolen gegevens worden doorverkocht?*

Er zijn twee belangrijke factoren die de waarde van gestolen laptops bepalen. Ten eerste is er de aankoopprijs, de waarde van een gebruikte laptop (gestolen of niet) ten opzichte van de kosten van een nieuwe. Hardware is goedkoper geworden, en gebruikte of gestolen apparatuur dus ook. In tegenstelling tot deze daling van de waarde van tweedehands apparatuur is internet als verkoopmedium opgekomen. Omdat internet zo'n efficiënt medium is om gebruikte of gestolen waren te verkopen, blijft de waarde voor de dief relatief hoog. Al met al is een gestolen laptop tegenwoordig beter te verkopen dan 10 jaar geleden, toen heling nog persoonlijk moest gebeuren met alle risico's van dien.

De kosten

Het is waarschijnlijk een troostrijke gedachte voor de meeste ICT-managers dat een gestolen laptop meestal opnieuw wordt geformatteerd en een nieuw besturingssysteem krijgt. Maar in een operationele context beginnen de problemen dan pas. Onderzoek van IDC wijst uit dat 58% van de kosten van de diefstal van een laptop niet in de hardware zit, maar in het verlies van intellectueel eigendom.

Toename van diefstallen van laptops in Europa

Om de toename van laptopdiefstallen te begrijpen moet een aantal factoren in overweging worden genomen. De toename wordt deels veroorzaakt doordat er veel meer laptops in gebruik zijn. Veel meer soorten medewerkers gebruiken ze. Laptops zijn niet langer beperkt tot bedrijfsruimtes op luchthavens en conferentiezalen in hotels. Ze worden gebruikt voor verkoop, technische taken, logistieke ondersteuning, enquêtes en trainingen. Deze veel bredere toepassing van de laptop in allerlei omgevingen met een hoger risico maakt hem kwetsbaarder voor diefstal.

IDC voorspelt dat de groei in de verspreiding van laptops 23% zal zijn in 2007 en dat de groei in 2008 nog steeds 21% bedraagt. Deze groei wordt aangejaagd door de vraag naar laptops als ondersteuning voor een steeds grotere groep taken. Vergelijkbare groeicijfers worden elders in de wereld gemeld.

De veiligheid van medewerkers

De mobiele telefoon is al een tijdje onderwerp van debat als het gaat om de veiligheid van medewerkers. Zijn medewerkers veiliger als ze kunnen bellen in geval van nood? Of zijn ze juist minder veilig, omdat ze het doelwit worden van overvallen en diefstal? Dit debat gaat natuurlijk gewoon verder. De laptop maakt de medewerker helemaal niet veiliger. Integendeel, als u zich een confrontatie met een dief voorstelt, wordt de veiligheid van de medewerker juist in gevaar gebracht.

De werkgever heeft waarschijnlijk een juridische, maar in ieder geval een morele plicht de medewerker in dergelijke situaties te beschermen. Maar wat kan de werkgever doen?

- Geef medewerkers een koffer die onopvallend is of gemakkelijk te verbergen is tijdens het reizen.
- Doe er een kabelslot bij en druk medewerkers op het hart hun apparatuur in de gaten te houden.
- Bied training aan over veiligheid of breng het op een andere manier onder de aandacht.
- Bedenk welke middelen van vervoer geschikt zijn voor een bepaalde omgeving of plaats.

Hierdoor voldoet een werkgever niet alleen beter aan zijn verplichtingen, maar loopt die ook minder kans waardevolle gegevens te verliezen.

Diefstal van laptops en het Europese midden- en kleinbedrijf

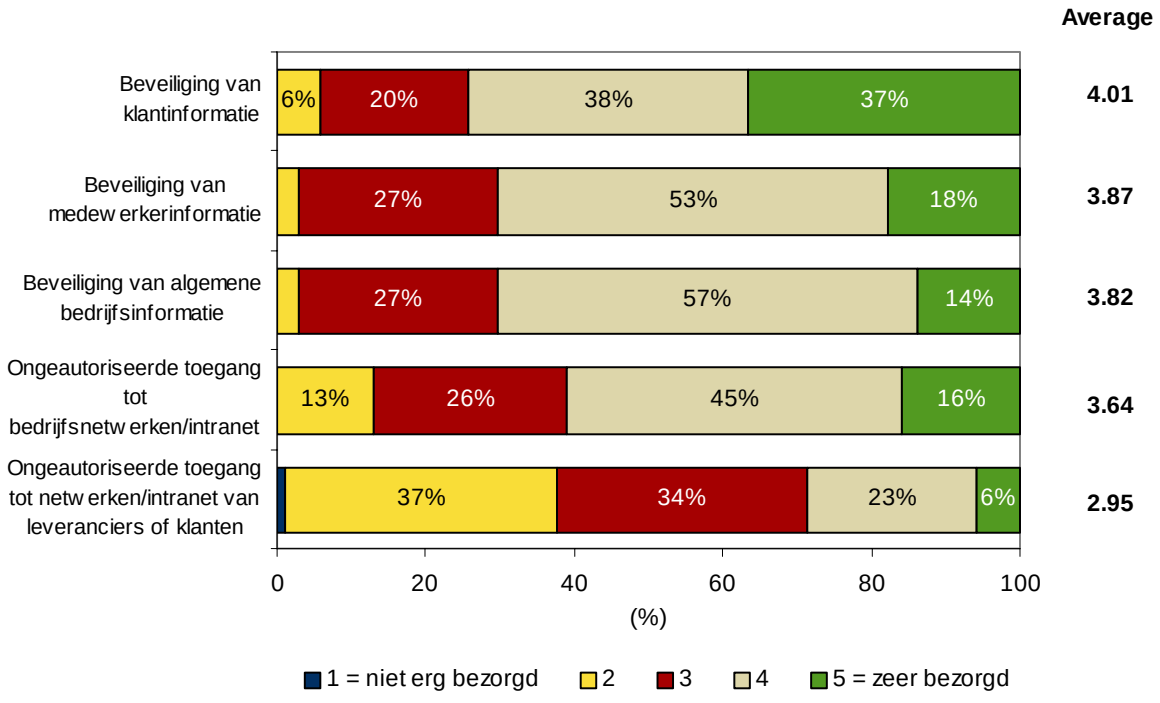
Diefstal van een laptop heeft voor het midden- en kleinbedrijf waarschijnlijk meer gevolgen dan als een vergelijkbaar apparaat van een groter bedrijf wordt ontvreemd: meer medewerkers die meerdere taken uitvoeren betekent meer computers die meerdere taken uitvoeren. Het resultaat is meer gegevens op diverse bedrijfsprocessen betrekking hebben. Dat betekent een groter verlies en blijvende financiële gevolgen.

De grootste zorg van vertegenwoordigers van het Europese midden- en kleinbedrijf is het verlies van klantgegevens. Het verlies van het vertrouwen van klanten wordt genoemd als het grootste risico van gegevensdiefstal.

FIGUUR 1

Diefstal van laptops: Belangrijkste zorgpunten

Vr. Als uw laptop wordt gestolen, geef dan voor elk zorgpunt uw mate van bezorgdheid aan...



Opmerking: n=200

Bron: IDC, 2007

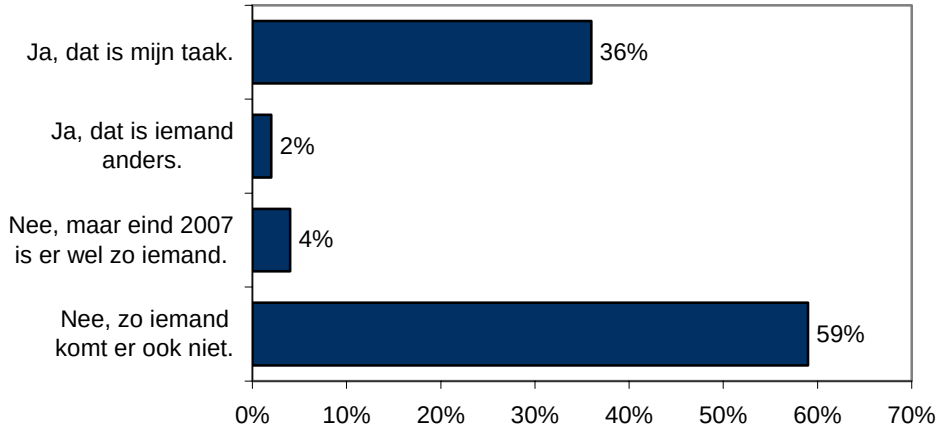
Dit moet worden gezien in het kader van een minder uitgewerkt beveiligingsbeleid en minder middelen waarover de extra werkbelasting kan worden verdeeld. Het is duidelijk dat het midden- en kleinbedrijf zichzelf moet beschermen tegen een dergelijk verlies. Voorkomen is tenslotte beter dan genezen.

Het is echter te verwachten dat het midden- en kleinbedrijf dezelfde benadering kiest als de consument. Met zijn beperkte gespecialiseerde beveiligingsinstrumenten en beperkt gebruik van versleuteling en softwarebeveiliging is het midden- en kleinbedrijf kwetsbaar voor diefstal. De meeste bedrijven in deze sector hebben geen eigen ICT-afdeling.

FIGUUR 2

Aanwezigheid beveiligingsfunctionaris

Vr. Heeft uw organisatie een gemeenschappelijke ICT-functionaris of een persoon die verantwoordelijk is voor de ICT-beveiliging?



Opmerking: n=200

Bron: IDC, 2007

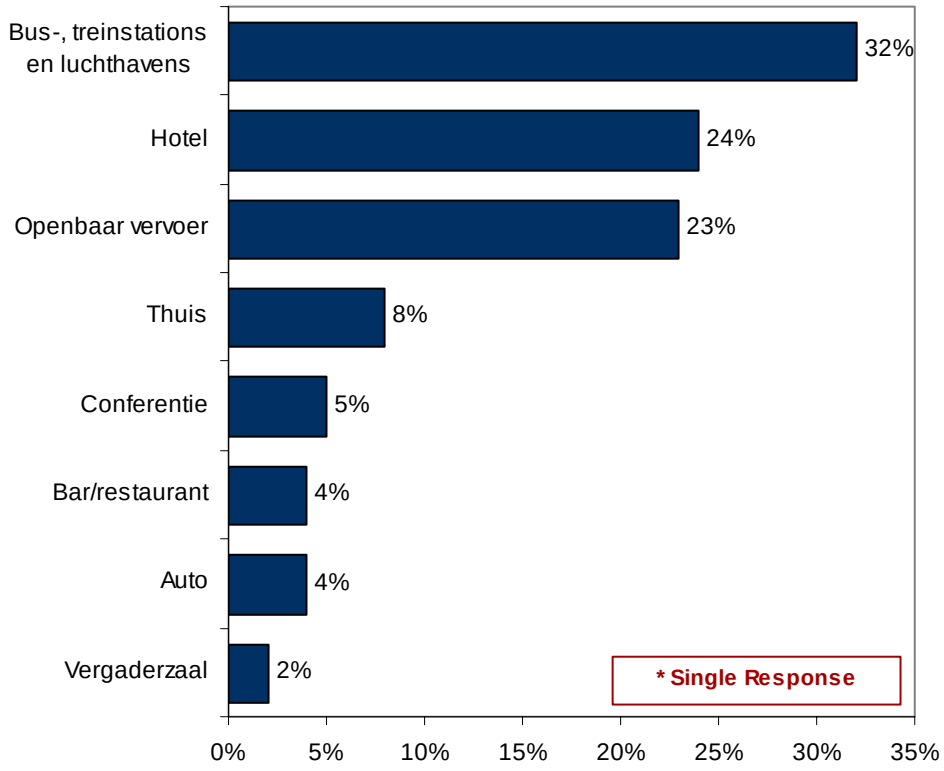
Wat is de omvang van het probleem?

Het onderzoek van IDC toont aan dat 92% van het Europese midden- en kleinbedrijf met mobiele medewerkers diefstal van laptops heeft meegemaakt. Gemiddeld komt dit eens in de 251 dagen voor en 54% van de bedrijven in deze sector hebben het afgelopen half jaar met diefstal te maken gehad.

FIGUUR 3

Risicogebieden

*Q. Op welke plaatsen is de kans op diefstal van één losse laptop het **meest waarschijnlijk***?*



Opmerking: n=200

Bron: IDC, 2007

Zoals te zien is in Figuur 3, komt diefstal van laptops op allerlei plaatsen voor, maar met name in het openbaar vervoer en in hotels.

Ook op de werkvloer wordt gestolen: 26% van de ICT-managers verdenkt eigen medewerkers van betrokkenheid bij diefstal en slechts 35% van de diefstallen op kantoor gaat vergezeld van inbraak. Veel dieven wandelen gewoon naar binnen: 31% van de ICT-managers die ervaring heeft met diefstal op kantoor zeggen dat ze dit hebben meegemaakt.

Invloed op de organisatie

Wat is de invloed op het midden- en kleinbedrijf?

Als er een laptop wordt gestolen, zijn er een aantal punten van zorg, waarvan de meest voor de hand liggende gewoonlijk niet zo ernstig zijn. We kunnen aantonen dat laptops zelden worden gestolen voor de gegevens. De lage hardwarekosten werden al genoemd. De echte kosten voor het bedrijf zitten in:

- Verlies van productiviteit van de gebruiker
- Verlies van vertrouwen van de klant
- Gemiste orders, ontbreken van productspecificaties, facturen e.d.
- Vertraagde facturering en betaling
- Verspilling van reis- en verblijfkosten

Al deze factoren zorgen dat de verliezen veel hoger uitvallen dan de kosten van het apparaat en de gegevens.

We weten uit Figuur 1 dat het midden- en kleinbedrijf het verlies van klantgegevens het meest vreest. En met reden. We hebben recentelijk vernomen dat een Britse financiële instelling een boete van £2,5 miljoen heeft gekregen voor het verlies van klantgegevens. Dit zou het einde van veel kleinere bedrijven betekenen. Als er geen regulerende instantie was, zou het verlies van vertrouwen van klanten veel moeilijker te dragen zijn. Kleinere bedrijven hebben niet altijd handige PR-functionarissen en ze hebben geen middelen om de onvermijdelijke fluctuaties in werkbelasting in bijvoorbeeld contactcentra op te vangen.

Het kan een kleiner bedrijf verscheidene dagen kosten gestolen hardware te vervangen. Vaak is men afhankelijk van extern personeel voor het beheer en het instellen van de pc. Ze hebben dus niet altijd de middelen en ook geen hardware op voorraad. En de gebruiker kan al die tijd niet werken, wat weer extra geld kost.

Achter de laptop

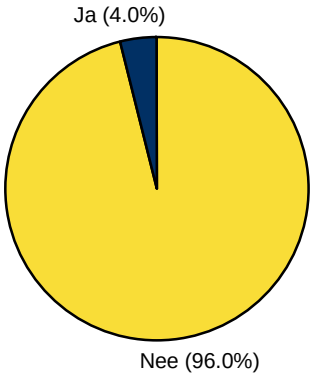
Het midden- en kleinbedrijf heeft tegenwoordig een infrastructuur die kortgeleden nog was voorbehouden aan grote bedrijven. Intranetten en VPN's zijn nu binnen het bereik van kleinere bedrijven gekomen en dit betekent een nieuw punt van zorg. De netwerken zijn wel professioneel, maar de beveiligingsmaatregelen en (nog belangrijker) het beveiligingsbeleid lopen vaak nogal achter. De diefstal van een laptop kan op deze manier de beveiliging van het netwerk in gevaar brengen.

Sommige laptops worden gebruikt om gegevens op het netwerk te benaderen, waarbij gevoelig materiaal in de cache aanwezig blijft. Soms maakt de gebruiker ook een lokale kopie voor eigen gebruik. Een andere mogelijkheid is dat een laptop wachtwoorden kan bevatten voor externe toegang tot een netwerk. Dit kan leiden tot grote en soms niet te detecteren schade.

FIGUUR 4

Downtime

Q. Vr. Houdt u de kosten van downtime door het vervangen van laptops bij?



Opmerking:n=200

Bron: IDC, 2007

Figuur 4 vertelt veel meer dan alleen de statistische kant. De meeste midden- en kleinbedrijven hebben geen idee van de totale kosten van de diefstal van een laptop voor hun bedrijf.

De exacte kosten berekenen is misschien minder belangrijk dan beseffen dat de kosten veel verder gaan dan het vervangen van de hardware. De gevolgen voor de veiligheid van de medewerker, kosten van het vervangen van de gegevens en het verlies van vertrouwen van de klant zijn allemaal factoren die moeten worden overwogen. Dit geldt zeker bij het formuleren van beleid en het regelen van interne trainingen en informatievoorziening om diefstal te voorkomen en het bewustzijn te verhogen.

Beveiligingsmaatregelen

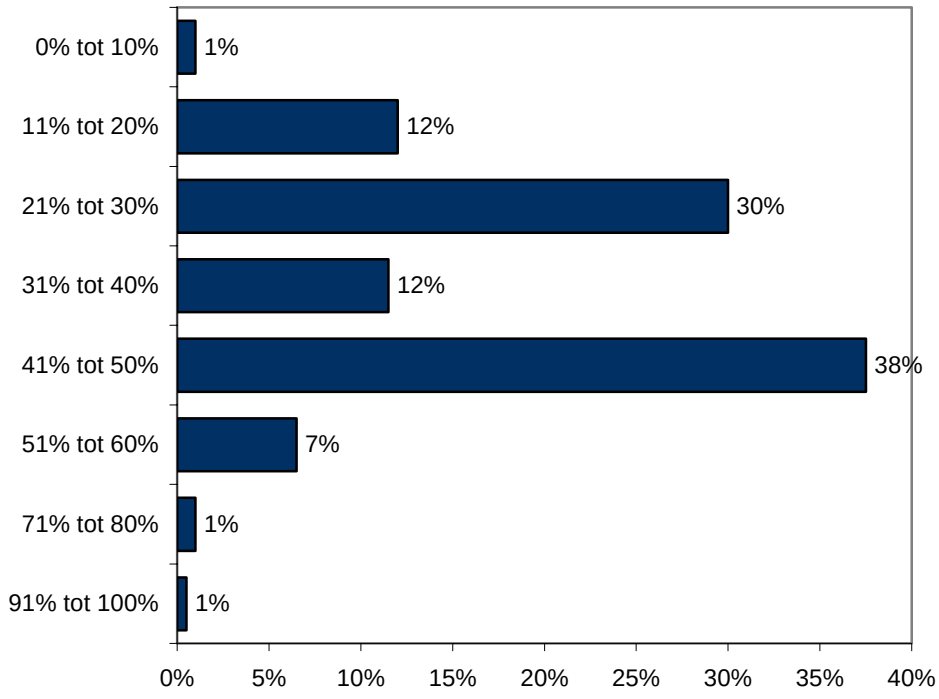
Er zijn heel wat producten op de markt voor de beveiliging van laptops: de vertrouwde kabelsloten en nieuwe opsporingsdiensten via internet hebben allemaal hun eigen plaats. Op de vraag wat ze zoeken in een beveiligingsproduct, noemden midden- en kleinbedrijven in Europa de volgende criteria, gerangschikt volgens belangrijkheid:

- Bewezen resultaten
- Productkwaliteit
- Gebruiksgemak

FIGUUR 5

Diefstalpreventie

Vr. Hoeveel procent van de diefstallen van laptops had kunnen worden voorkomen met een kabelslot?



Opmerking: n=200

Bron: IDC, 2007

Figuur 5 laat zien dat het Europese midden- en kleinbedrijf ervan overtuigd is dat fysieke beveiliging meer waar voor zijn geld biedt dan software-oplossingen.

ICT-managers in Europa geloven dat 40% van de diefstallen van laptops had kunnen worden voorkomen als een kabelslot was gebruikt.

Aanbevolen handelswijzen

IDC raadt organisaties aan voor de beveiliging van laptops de volgende punten aan te pakken en er beleid voor te formuleren:

- Een methode om het bewustzijn te verbeteren en de frequentie van campagnes
- Richtlijnen voor de fysieke bescherming van laptops
- Frequentie en methode van back-ups van gebruikersgegevens
- Indeling van gegevenstypen als extern of niet extern te gebruiken op basis van risico/voordeel
- Externe toegang of toegang via een VPN van niet-externe gegevenstypen en -bronnen beperken
- Fysieke beveiliging
- Zichtbare afschrikking
- Beveiliging van gegevens
- Koffers en vervoerswijzen

Er moeten ook richtlijnen voor gebruikers komen met de volgende punten:

- Laptop altijd vergrendelen
- Laptops altijd uit zicht houden (niet op een autostoel, bij een raam enz.)
- Regelmatig back-ups maken
- Bewust zijn van risico's op openbare plaatsen
- Bewust zijn van het gevaar van het rondlopen met draagbare computerapparatuur.

Conclusie

De beveiliging van laptops is iets dat elk Europees midden- en kleinbedrijf serieus zou moeten nemen. Het gebruik van mobiele computers neemt toe en het beveiligingsbeleid moet meegroeien.

Mobiele werkplekken ontwikkelen zich voortdurend. Het beveiligingsbeleid moet daarom constant worden geëvalueerd en aangepast. Beveiliging moet niet alleen inspringen op elke nieuwe bedreiging, maar de beveiliging van mobiele werkplekken moet een integrale overweging zijn bij alle stadia van de ontwikkeling van de mobiele medewerkers en hun instrumenten.

Er moet aandacht zijn voor nieuwe en innovatieve beveiligingsproducten en hardware naast de oude vertrouwde fysieke bescherming zoals kabelsloten in de strijd tegen de verstoring van bedrijfsprocessen die het gevolg zijn van de diefstal van mobiele apparatuur.

Auteursrechtvermelding

Neem voor meer informatie over dit document contact op met:

Marketingafdeling

Tel: +44 (0) 20 8987 7100

IDC is a subsidiary of IDG, one of the world's top information technology media, research and exposition companies.

Visit us on the Web at www.idc.com

To view a list of IDC offices worldwide, visit www.idc.com/offices