

Beveiligings, bewustzijnsonderzoek

November 2010

.....
‘31% van de inbreuk op gegevens vindt plaats door frustraties voortvloeiende uit het IT-beveiligingsbeleid waardoor werknemers hun werk niet kunnen doen’
.....

Voorwoord



Richard Turner
Algemeen directeur

Het doet met veel plezier dit wereldwijde onderzoeksproject te mogen introduceren dat Clearswift heeft uitgevoerd om het IT-beveiligingsbeleid binnen bedrijven te onderzoeken.

Dit rapport vloeit voort uit de zeer succesvolle reeks rapporten die verscheen in april 2010 en de houding van bedrijven onderzocht ten aanzien van Web 2.0-technologieën en het gebruik van dergelijke hulpmiddelen op de werkplek.

De resultaten van het oorspronkelijke onderzoek laten een belangrijke mentaliteitsverandering bij bedrijven zien, wat duidelijk maakt dat bedrijven op dit moment Web 2.0 en andere gezamenlijke technologieën accepteren welke cruciaal zijn voor het toekomstige succes van hun bedrijf.

Maar terwijl het IT-landschap van bedrijven steeds complexer wordt en snelle verandert als gevolg van de veranderingen die Web 2.0 technologieën met zich meebrengen, hoe bereid zijn bedrijven dan, en nog belangrijker, hoe bereid zijn hun werknemers, om de daaruit voortvloeiende uitdagingen op beveiligingsgebied aan te gaan?

Dit nieuwe onderzoek gaat verder en onderzoekt de houding ten aanzien van het IT-beleid in bedrijven over de hele wereld. De resultaten zijn zowel boeiend als tot nadenken stemmend.

Een bijzonder interessante bevinding is het klaarblijkelijke gebrek aan opleiding van werknemers als het gaat om IT-beleid - veel medewerkers krijgen alleen een opleiding wanneer ze bij het bedrijf in dienst treden, maar met technologie die zó snel verandert, is dit duidelijk verre van ideaal. De realiteit is dat de werknemers een essentieel onderdeel kunnen vormen van de gegevensbescherming en informatiebeveiliging binnen een bedrijf. Ervoor zorgen dat het personeel het beleid kent en begrijpt kan een enorm voordeel opleveren voor bedrijven.

IT-beveiligingsbedrijven hebben te lang geprofiteerd van het feit dat hun klanten zich onzeker voelen en daarbij ingespeeld op angsten en negatieve gevoelens om de winst te maximaliseren. Het is mij duidelijk dat met het oog op meer veiligheid, bedrijven zich op de eerst plaats niet langer onzeker moeten voelen.

Mijn belangrijkste boodschap op basis van dit rapport is simpel - IT-beveiliging moet vanuit de donkere krochten van de IT-afdeling aan het daglicht treden en duidelijk zichtbaar worden gemaakt binnen de organisatie. Met een relevant en actueel beveiligingsbeleid kan een onderneming zijn werknemers het werk laten doen dat ze moeten doen en voor productiviteit en innovatie zorgen.

A handwritten signature in black ink, appearing to be 'R. Turner', written over a horizontal line.

Kerngegevens

- 71% van de kantoormedewerkers zegt dat het bedrijf een duidelijke internetbeleid heeft dat de meeste werknemers begrijpen.
- 50% van de kantoormedewerkers heeft in de laatste 12 maanden het internetbeleid met collega's besproken, maar slechts 29% heeft een relevante opleiding in het onderwerp gehad gedurende deze periode
- 22% weet niet of hun internetgebruik wordt gecontroleerd op het werk
- Slechts 15% van de kantoormedewerkers maakt zich zorgen dat ze onbedoeld het veiligheidsbeleid schenden - maar inbreuken op de veiligheid worden het meest toegeschreven aan onwetendheid/ gebrek aan inzicht (63%)

.....

Resultaten van de Clearswift Security Awareness Survey zijn gebaseerd op 2000 online-interviews met kantoormedewerkers in het VK, de VS, Australië, Duitsland en Nederland.

Het onderzoek werd uitgevoerd door Loudhouse, een onafhankelijk marktonderzoekadviesbureau dat is gevestigd in Londen

.....

Samenvatting

Nu de technologie voor het delen van informatie meer en meer ingebed wordt in ons leven, wordt het voor mensen met toegang tot de gegevens op de werkplek steeds belangrijker om te begrijpen welk gebruik van gegevens is toegestaan en welke activiteiten die gegevens in gevaar kunnen brengen.

De Clearswift Security Awareness Survey onderzoekt de mate waarin kantoormedewerkers de implicaties van hun dagelijkse activiteiten voor de gegevensbeveiliging begrijpen en legt een interessant fenomeen onder kantoormedewerkers bloot wat gegevensbeveiliging betreft. Het blijkt dat werknemers in een kantooromgeving een misplaatst vertrouwen hebben in hun eigen niveau van inzicht en niet altijd zijn uitgerust met de kennis die ze nodig hebben om gegevens veilig op te slaan. Als zodanig kan de beveiliging van gegevens worden beschouwd als een "onbekende grootheid" - werknemers die denken dat ze de gegevensbeveiliging begrijpen, zijn zich niet bewust van het feit dat ze meer informatie en begeleiding nodig hebben.

Overmoed kan dus als de belangrijkste bedreiging van gegevensbeveiliging in de hedendaagse kantooromgeving worden gezien. Medewerkers zijn ervan overtuigd dat ze begrijpen wat veilig is en wat toegestaan is, en dit leidt bij velen tot een wat nonchalante houding ten opzichte van IT in het algemeen, vaak doen ze "er wel erg gemakkelijk" over en verplaatsen gegevens blindelings van de ene plek naar de andere zonder rekening te houden met de potentiële veiligheidsrisico's. Deze situatie wordt nog eens verergerd door het feit dat er een gebrek is aan consistente communicatie over het veiligheidsbeleid, en dus veel kantoormedewerkers dit niet in zijn volledigheid begrijpen. Ondanks het feit dat de meerderheid van de kantoormedewerkers zichzelf in deze enquête als risicoafwijzend zien, stellen ze individueel en collectief hun werkgevers onbedoeld toch bloot aan gegevensbeveiligingsrisico's.

Teneinde het gebruik van best practices in de gegevenbeveiliging te bevorderen, raadt Clearswift werkgevers aan om hun werknemers actief te betrekken bij een dialoog over veiligheid, verantwoordelijkheid en risico.



.....

‘Technologie voor het delen van informatie raakt meer en meer ingebed in ons leven’

.....

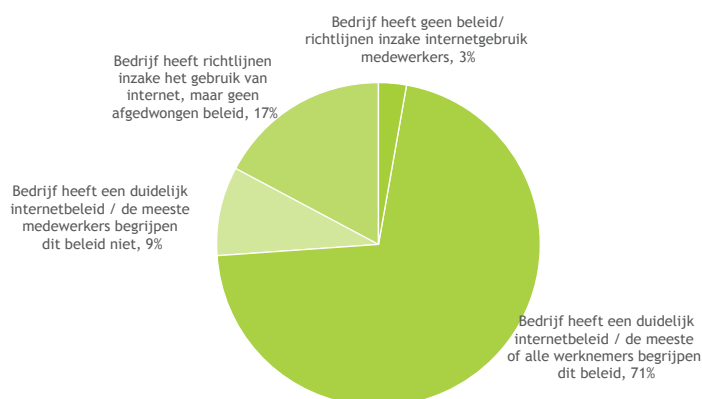
Het beleid in de praktijk

Nu internet voor velen een alomtegenwoordige deel van het beroepsleven is gaan vormen, is het niet verwonderlijk dat de meeste werkgevers een internetbeleid hebben. 71% zegt zelfs niet alleen dat hun werkgever een dergelijk beleid heeft, maar dat de meeste collega's dit beleid ook begrijpen. Slechts 20% zegt dat hun bedrijf helemaal geen officieel beleid heeft. Bovendien wordt dit beleid door het grootste deel van de werknemers als eerlijk en begrijpelijk beschouwd - slechts 10% zien de regels van hun werkgevers als oneerlijk en slechts 8% is van mening dat het beleid van de werkgever geen zin heeft.

Ondanks het bestaan van een internetbeleid en naar zeggen een hoog begrip voor een dergelijk beleid onder kantoormedewerkers, is een geformaliseerde communicatie rond het internetbeleid in het slechtste geval niet-bestaand en in het beste geval zeer fragmentarisch. Hoewel het gebruik van het internetbeleid een onderwerp kan zijn van "koffieautomaat"-gesprekken, laat afbeelding 2 zien dat de helft van de kantoormedewerkers (50%) de afgelopen 12 maanden een gesprek over het internetgebruiksbeleid heeft gevoerd. In tegenstelling daarmee heeft slechts 29% in die periode een speciale training gehad in dit beleid, en slechts 14% heeft een vraag gesteld om te controleren of iets wat ze deden ook was toegestaan op grond van het bedrijfsbeleid. Sterker nog, de helft van de respondenten had nog nooit een speciale training genoten in het huidige bedrijfsveiligheidsbeleid. En nóg sterker, 38% had helemaal geen opleiding gehad in veiligheidsvraagstukken in hun huidige baan (tijdens een speciale sessie of anderszins.) Dit suggereert dat zelfs degenen die enige training hebben genoten (bij hun indiensttreding of tijdens een geplande sessie), geen up-to-date informatie krijgen wanneer ze zich door hun organisaties verplaatsen.

Werknemers meent dat hun bedrijf pro-actief moet zijn in veiligheidsaangelegenheden - 58% meent dat hun werkgever zijn werknemers pro-actief aanmoedigt om het beleid te begrijpen, en in het algemeen zien ze dit beleid als goedbedoeld, maar het is duidelijk dat de kloof tussen goede bedoelingen en concrete actie voor veel werkgevers groot is.

Afbeelding 1: Bestaan van en inzicht in het internetbeleid van het bedrijf



Afbeelding 2: Communicatie over internetbeveiliging



.....

‘werknemers begrijpen het toegepaste beleid’

.....

Er wordt verwarring nageleefd

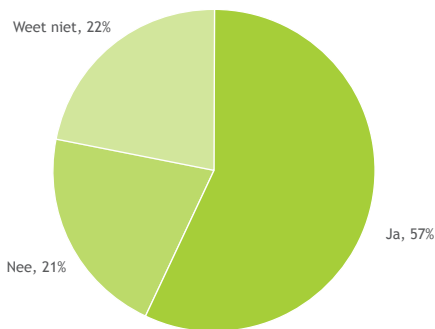
De meerderheid van de kantoormedewerkers beweert dat men het internetbeleid van hun werkgevers in grote lijnen begrijpt, maar nog wel verward is over bepaalde aspecten van dat beleid. Toezicht op het internetgebruik op het werk geeft de meeste verwarring: 21% zegt dat elektronisch toezicht door hun werkgever het meest verwarrende aspect van het internetgebruik op het werk is. Afbeelding 3 laat zien dat meer dan 1 op de 5 kantoormedewerkers (22%) niet weet of hun internetgebruik op het werk wordt gecontroleerd. Van degenen (57%) die weten dat hun internetgebruik op het werk wordt gecontroleerd, denkt 38% dat de mate van toegang door hun werkgever tot informatie over persoonlijke internetgebruik hoger dan noodzakelijk is om de veiligheid te handhaven. Zoals een respondent zei *“Niemand weet precies wie de internetactiviteit ziet en wat voor soort informatie in de rapporten staat, hoe vaak het is bekeken en verspreid.”*

Afbeelding 4 laat het inzicht van kantoormedewerkers in gegevensbeveiligingsonderwerpen zien. Het vertrouwen is het hoogst bij het inzicht in welke gegevens via e-mail kunnen worden verzonden (79% heeft er vertrouwen in), wat wel en niet mag op aan het werk gerelateerde sociale media (65%), en lager wat betreft het inzicht in de veiligheid van met het werk samenhangende e-mails (52%).

Andere gegevensbeveiligingsterreinen die verwarring veroorzaken onder werknemers hebben betrekking op:

- Wie heeft toegang tot de gegevens over mijn internetgebruik op het werk
- Welke gegevens kan ik delen met mensen in andere functies en op andere afdelingen
- Welke gegevens mag ik buiten het werk delen
- Wat mag ik zeggen over het werk van anderen
- Met wie mag ik communiceren wanneer ik aan het werk ben

Afbeelding 3: Internettoezicht op het werk
Mijn internetgebruik op het werk wordt elektronisch gecontroleerd door mijn werkgever



38% vindt dat werkgever informatie over personeel online-activiteiten meer dan noodzakelijk bekijkt om de veiligheid te waarborgen

1 op 5 (22%) vindt dat de werkgever persoonlijke online-activiteiten meer dan noodzakelijk bekijkt om de veiligheid te waarborgen

Afbeelding 4: Werknemersvertrouwen rond gegevensbeveiligingskwesties



Het toezicht op het internetgebruik op het werk zorgt voor de meeste onduidelijkheid'

Nonchalante naleving

Interessant genoeg maakt, hoewel de persoonlijke vertrouwensniveaus in gegevensbeveiliging hoog zijn - slechts 15% van de kantoormedewerkers zich zorgen over het feit dat ze door hun internetgebruik onbedoeld het veiligheidsbeleid overtreden -

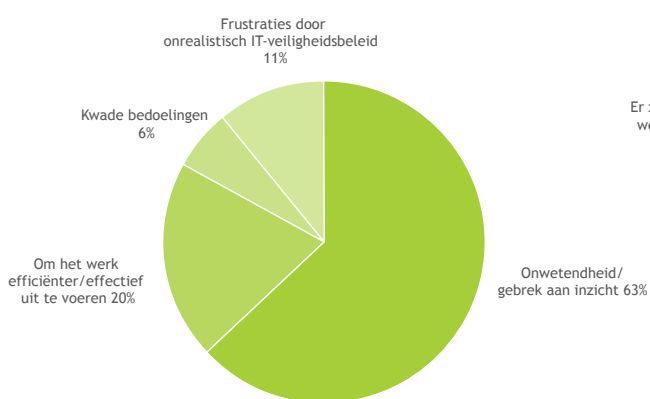
63% van de kantoormedewerkers wijt het merendeel van de inbreuken op de veiligheid aan onwetendheid of een gebrek aan inzicht [afbeelding 5] Het lijkt daarom dat kantoormedewerkers de neiging hebben om hun eigen begripsniveau van gegevensveiligheidsaangelegenheden hoger aan te slaan dan dat van de andere medewerkers! Het is ook opvallend dat 1 op de 5 mensen denkt dat inbreuken op de veiligheid plaatsvinden om het werk efficiënter en effectiever gedaan te krijgen, terwijl 11% denkt dat het te maken heeft met frustraties door een onrealistisch IT-veiligheidsbeleid.

Een deel van het probleem lijkt voort te vloeien uit een houding van 'nonchalante' naleving.

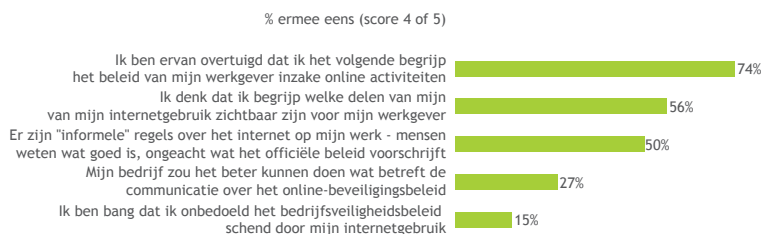
Kantoorcommunicatie kan worden vergeleken met het oude doorvertelspel, waarbij de helft van de kantoorwerkers (50%) meldt dat er informele regels over het internet op het werk bestaan en dat de meeste mensen begrijpen wat acceptabel is, ongeacht wat het officiële beleid zegt [afbeelding 6] Zonder training en een consistente, up-to-date communicatie over het bedrijfsbeleid, vervagen de scheidslijnen tussen deze informele normen en het feitelijke beleid en worden de bedrijfsgegevens blootgesteld.

Aangezien slechts 27% van de kantoormedewerkers denkt dat hun bedrijf de communicatie over het online-beveiligingsbeleid zou kunnen verbeteren, lijkt het erop dat veel mensen niet echt over veiligheid nadenken en het niet bovenaan op hun agenda staat bij de dagelijkse besommeringen. Deze fragmentarische vertrouwensniveaus rond de gegevensbeveiliging illustreren eens te meer dat er een idee van misplaatst vertrouwen heeft postgevat bij zowel werknemers als werkgevers, en geven het belang aan van een vollediger en frequentere communicatie naar de werknemers toe.

Afbeelding 5: Redenen waarom IT-beveiliging wordt geschonden



Figuur 6: Nonchalante naleving onder kantoormedewerkers



'1 op de 5 mensen denkt dat inbreuk plaatsvindt om het werk efficiënter en effectiever te laten verlopen'

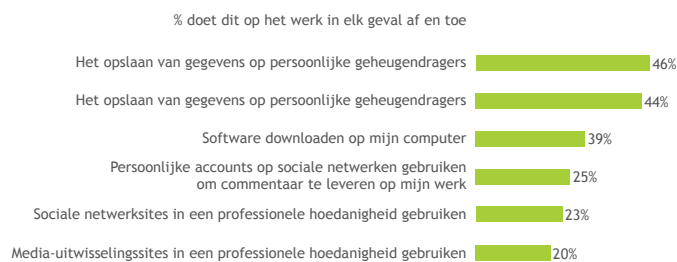
Luchtig met IT

Kantoormedewerkers over de hele wereld gebruiken een heel scala van technologieën om hun werk te doen en hun persoonlijke leven te runnen. De grenzen tussen werk en thuisgebruik en juiste en onjuist technologiegebruik veranderen steeds en zijn in essentie onduidelijk. Afbeelding 5 laat enkele voorbeelden zien waarbij kantoormedewerkers erg luchtig omgaan met de IT en hun eigen regels over technologiegebruik toepassen, ongeacht wat het officiële beleid voorschrijft. 44% van de kantoormedewerkers meldt werkgerelateerde gegevens op te slaan op persoonlijke geheugendragers, 39% downloadt software op hun computer op het werk en 25% gebruikt persoonlijke accounts op sociale netwerken voor commentaar op hun werk. Zoals een geënquêteerde het stelde: *“Ik open mijn persoonlijke e-mailaccounts en doe ook aankopen tijdens mijn lunchpauze. Ik hoop echt dat niemand mijn creditcardgegevens kan zien of mijn e-mails kan lezen”*.

De meeste van de dagelijkse online-activiteiten is waarschijnlijk persoonlijk, aangezien slechts 14% gebruik maakt van sociale media voor werkdoeleinden (dat wil zeggen, bijdragen leveren aan Facebook, Twitter, LinkedIn, of een andere sociale website als onderdeel van hun functiebeschrijving). E-mail domineert nog steeds de werkcommunicatie en veel van deze e-mails wordt gehost in de wolk, waardoor er beveiligingsproblemen ontstaan waarvan medewerkers zich helemaal niet bewust zijn. 74% gebruikt vaak e-mail en andere webgebaseerde media om met klanten of cliënten over zaken te communiceren.

Kortom, kantoormedewerkers gebruiken op regelmatige basis een verscheidenheid aan technologieën met uiteenlopende risiconiveaus. Het feit dat kantoormedewerkers erop blijven vertrouwen dat ze voldoen aan het gegevensbeveiligingsbeleid bij afwezigheid van een formele training in dergelijke aangelegenheden, is een reden tot bezorgdheid. Deze situatie is op de lange termijn duidelijk onhoudbaar nu de bedreigingen op het gebied van gegevensbescherming steeds diverser en verfijnder worden, technologie steeds mobieler wordt en de scheidslijnen tussen privé en zakelijk vervagen.

Afbeelding 7: Voorbeelden van luchtig omgaan met IT



‘kantoormedewerkers gaan in wezen heel luchtig om met IT’

Samenvattend

Het is duidelijk dat hoewel medewerkers ervan overtuigd zijn dat ze het beveiligingsbeleid van hun werkgevers begrijpen, dit vertrouwen vaak onterecht is. Kennis wordt te vaak informeel overgedragen door middel van gesprekken tussen medewerkers en uitgehard tot informele richtlijnen die het feitelijke gegevensbeschermingsbeleid vervangen bij afwezigheid van training.

Door een luchtige omgang met IT vervagen de scheidslijnen tussen persoonlijke en werktechnologie, ontstaan er risico's wanneer gevoelige bedrijfsgegevens worden opgeslagen op persoonlijke USB-sticks en persoonlijke informatie via werklaptops wordt verzonden.

Deze situatie is zeer riskant op de lange termijn, zowel voor werkgevers (die mogelijk lijden onder de gevolgen wanneer de werknemers de regels overtreden) en werknemers (die mogelijk onbedoeld persoonlijke informatie onthullen via werkplekcontrole of hun carrière op het spel zetten.) Er zijn echter hoge niveaus aan goodwill binnen organisaties en hier kan gebruik van worden gemaakt om deze beveiligingskloof te dichten.

De meest vooruitstrevende organisaties moeten hun beveiligingskloof dichten door twee problemen tegelijk aan te pakken. Technologische oplossingen kunnen de gegevens onder controle helpen houden door de handhaving te automatiseren en de risico's te beperken. Naast deze oplossingen is echter regelmatig training nodig, zodat de werknemers met vertrouwen met de bescherming van gevoelige gegevens op het werk om kunnen gaan.

Contact Clearswift



Verenigd Koninkrijk
1310 Waterside,
Arlington Business Park,
Theale,
Reading,
Berkshire,
RG7 4SA

Tel.: +44 (0) 11 8903 8903
Fax: +44 (0) 11 8903 9000

Nederland
Marcel Koorling
Tel.: +31 6 204 35 239
Marcel.Koorling@clearswift.com