

# Nieuwsbrief

## 04

### In deze Nieuwsbrief

- > Uw persoonsgegevens ... Goed beschermd?
- > Applicatie Security ... Waarom?
- > Mensen hebben ook updates nodig!
- > Nieuwe wet Meldplicht Datalekken ... Bent u klaar?

### Uw persoonsgegevens ... Goed beschermd?

**Het is de afgelopen tijd weer erg onrustig geweest in security land. Berichten over security incidenten verschijnen nog steeds dagelijks in de media. Bij dergelijke incidenten komen regelmatig persoonsgegevens in handen van onbevoegden. Die gegevens worden dan misbruikt, verkocht en voor totaal andere doeleinden ingezet dan waarvoor ze eigenlijk werden opgeslagen. Oneigenlijk gebruik van data is zeer risicovol.**

Er ontstond daarom ook grote opschudding toen een grote bank bekend maakte dat ze de betalingsgegevens van hun klanten wilden gaan gebruiken voor marketing doeleinden. Na heftige reacties uit de markt is dat plan voorlopig even in de ijskast gezet. De implicaties van zo'n plan kunnen groot zijn. Het begint bij "reclame die beter gericht is op de doelgroep" maar dat zou zomaar uit de hand kunnen lopen als die data in handen komt van marketing organisaties die wat minder

### Applicatie Security... Waarom?

Heeft u uw webapplicaties wel eens laten controleren op security-kwetsbaarheden? Zo niet, dan is er een grote kans dat u een groot risico loopt op een digitale inbraak. Veel mensen blijven nog steeds denken dat een hackers-aanval een "ver van hun bed show" is. Ze vergeten daarbij dat "ver van mijn bed" niet van toepassing is op het internet.

Hackers werken tegenwoordig met geavanceerde tools waarmee ze in korte tijd grote aantallen webapplicaties (lees: websites) kunnen "controleren" op kwetsbaarheden. Ook uw website zit daarbij! Deze tools zijn makkelijk te verkrijgen via het internet.

In onze gesprekken met bedrijven horen we helaas nog veel te vaak: "Wij lopen echt geen gevaar, wat kunnen ze hier nou halen". Soms valt er inderdaad niets te halen. Maar dan kunnen hackers altijd nog wat brengen. Wat zou het gevolg

### Mensen hebben ook updates nodig!

In de media verschijnen regelmatig artikelen en blogs met tips voor het verlagen van de risico's op cybercrime. Vaak beperken deze tips zich tot min of meer technische zaken zoals bijvoorbeeld de instellingen van een systeem of applicatie. Vaak wordt het gedrag van de mensen hier niet bij genoemd. Bij het verlagen van de risico's op cybercrime is het belangrijk dat de gebruikers van de ICT middelen op zijn minst bewust zijn van de dreigingen.

Sebyde BV verzorgt regelmatig informatieve presentaties van 1,5 – 2 uur waarin de laatste stand van zaken wordt gepresenteerd op het gebied van Cybercrime, dreigingen en de mogelijke gevolgen. Deze sessies zijn absoluut niet technisch en bedoeld voor alle medewerkers van een organisatie. Het is een eye-opener voor velen en laat de mensen nadenken over de security aspecten op hun eigen werkplek.

### Nieuwe wet Meldplicht Datalekken : Bent u er klaar voor?

Vooruitlopend op de nieuwe Europese Privacywetgeving zal de bestaande wet Meldplicht Datalekken gaan gelden voor alle organisaties.

Zowel private als publieke organisaties die persoonsgegevens verwerken worden straks verplicht om inbreuken op de beveiliging die leiden tot diefstal, verlies of misbruik van persoonsgegevens binnen 72 uur te melden. Dat zijn dus meer organisaties dan de aanbieders van elektronische communicatienetwerken en -diensten voor wie op grond van de Telecommunicatiewet reeds een meldplicht geldt. Tevens heeft de toezichthouder (CBP, het College Bescherming

### Kunnen wij u helpen?

Bij de security van web applicaties (websites), netwerken en systemen.

Het trainen van medewerkers of developers op het gebied van security awareness.

Het doen van een Management workshop ter voorbereiding van het implementeren van een Security Awareness programma.

Het laten controleren van de mogelijke privacy impact van uw informatiesystemen en organisatie.

Neem contact op

netjes omgaan met de data. Denk niet dat er altijd verantwoord wordt omgegaan met uw data. In Engeland heeft de NHS (het Engelse Ziekenfonds) 49 miljoen patiëntgegevens verkocht aan een verzekeringsmaatschappij. Het gevolg was een verhoogde verzekeringspremie voor veel mensen.

Security is de verantwoordelijkheid van iedereen. Niet alleen technische oplossingen, maar zeker ook het gedrag van de mens en het inrichten van de juiste processen in een bedrijf bepalen de mate van risico wat wordt gelopen.

Sebyde helpt. Van het verhogen van het bewustzijn (training) tot het inrichten van een Security awareness programma en het controleren van systemen en applicaties. Neem [contact](#) op over hoe Sebyde u hierbij kan helpen.

kunnen zijn als de homepage van uw website ineens een pornografische afbeelding laat zien? Klanten en relaties zouden daardoor hun vertrouwen kunnen verliezen in uw bedrijf en weglopen. De schade (zowel financieel als reputatie!) is dan niet te overzien. Hackers kunnen Malware op uw netwerk plaatsen die op een later tijdstip hun verwoestende werk gaan uitvoeren.

Applicaties kunnen gecontroleerd worden op kwetsbaarheden. Een volledige scan door Sebyde BV van uw domein is 3 dagen werk en kost 3.495 Euro. Een "vital few scan" (scan op de 45 meest gevaarlijke kwetsbaarheden) kost 995 Euro. Relatief kleine investeringen waarmee u grote schade kunt voorkomen.

We beschikken over abonnementsvormen waarbij regelmatige scans worden uitgevoerd tegen zeer aantrekkelijke prijzen. Neem [contact](#) op over hoe Sebyde u hierbij kan helpen.

Deze sessies verzorgen we aan huis. Ideaal geschikt voor bedrijven, maar ook voor netwerkbijeenkomsten, Business clubs, verenigingen, etc.

De presentatie geeft een goed overzicht van de mogelijkheden die door hackers worden gebruikt om toegang te krijgen tot informatie. We laten filmpjes zien en geven veel voorbeelden. Er wordt ingegaan op de consequenties van het plaatsen van gegevens op Social Media. Tevens geven we een aantal handvatten ter vermindering van de risico's op de eigen werkplek.

De presentatie kost 49,50 Euro per persoon, minimaal 5 personen. Bij meer dan 10 personen speciale prijzen. Sommige bedrijven maken er een "Pizza-sessie" van die om 17.00 uur of later start. Wat ons betreft OK!

Vraag [informatie](#) aan over de Sebyde Security Awareness presentatie.

Persoonsgegevens) een uitbreiding gekregen van de bevoegdheid tot het opleggen van bestuurlijke boetes. Deze boetes zijn van materieel belang, 5% van uw wereldwijde jaaromzet met een maximum van 100 miljoen Euro (!)

Bedrijven dienen zich op deze wetgeving voor te bereiden. Sebyde BV helpt u bij het documenteren van de mogelijke privacy impact van de gebruikte systemen en applicaties.

Vraag [hier](#) informatie aan over de wet meldplicht datalekken en het Sebyde privacy onderzoek.

Telefoon +31 6 53 23 32 69

Email [rob.koch@sebyde.nl](mailto:rob.koch@sebyde.nl)

Website <http://www.sebyde.nl>

LinkedIn <http://www.linkedin.com/company/sebyde-bv>

Twitter <http://www.twitter.com/SebydeBV>

Facebook <http://www.facebook.com/sebydeBV>