Nieuwsbrief 02

In deze **Nieuwsbrief**

2014: Het jaar van de Privacy!

"2014 wordt een spannend jaar. Het is nu al door sommigen uitgeroepen als het jaar van de privacy. In de loop van 2014 zal de Wet meldplicht datalekken van kracht worden. Daarnaast zullen in 2014 de onderhandelingen over de Europese Privacy Verordening (EPV) afgerond worden."
(bron: Duthler & associates).

Beide wetgevingen hebben vergaande implicaties voor bedrijven en instellingen. Alleen al vanwege de hoogte van de boetes is naleving van de privacywetgeving een boardroom issue geworden. Nieuwe systemen zullen moeten voldoen aan het principe van "Privacy by Design", dat betekent dat de wetgeving moet zijn ingebouwd in de software, processen en de organisatie.

Ons advies is om het komende jaar hieraan serieus aandacht te besteden. Al was het maar omdat de aanstaande wetgeving er van uit gaat dat organisaties de huidige privacywetgeving op orde hebben. Bedrijven dienen zich nu voor te bereiden op de EPV anders zijn ze te laat.

Neem contact op over de mogelijkheden die er zijn om uw privacy- en Security situatie in kaart te brengen.

Voor meer informatie over het Sebyde Privacy onderzoek, lees verder.

Web Applicatie Security Scan

In de vorige nieuwsbrief, klik hier, hebben we 5 belangrijke redenen gegeven waarom het noodzakelijk is om software te laten testen op de kwetsbaarheden in de security. Het risico wat je loopt als websites kwetsbaarheden bevatten mag niet onderschat worden. Toch merken we dat dit risico door veel organisaties wordt onderschat.

Denk niet dat het u niet zal overkomen. Hackers vallen meestal niet gericht uw website aan. Ze gebruiken tools die duizenden websites nalopen op zwakke plekken Daar kan uw website dus zomaar tussen zitten. De gevolgen kunnen groot zijn. Het argument: "Ze komen hier echt niet hoor, wat valt hier nou te halen?" is tegenwoordig niet meer van toepassing.

Een scan van een website is snel en effectief. Na een intakegesprek voeren we de scan uit. 2 dagen later ontvangt u een uitgebreid rapport over de gevonden kwetsbaarheden, hoe ze veroorzaakt worden en (het belangrijkste!) een advies over hoe de gevonden kwetsbaarheden gerepareerd kunnen worden. Indien blijkt dat er géén high- of medium security kwetsbaarheden in de website zitten geven we het Sebyde keurmerk uit als bewijs dat de applicatie door ons gescand is en veilig is bevonden.

Voor meer informatie lees verder

Security Awareness

Hoeveel keer heeft u de afgelopen kerst en oud-nieuw periode geklikt op een wenskaart-email? Bewustzijn op het gebied van security is één van de belangrijkste factoren bij het verlagen van de risico's.

Je kunt als organisatie alles regelen om informatiesystemen met behulp van technische maatregelen te beschermen.

Als echter de medewerkers driftig blijven klikken op phishing mails, onveilige passwords gebruiken en die passwords ook nog eens op gele post-it briefjes op het beeldscherm plakken, dan blijft de organisatie erg kwetsbaar.

Er wordt nog vaak gedacht: "Als er iets misgaat dan hebben ze op de ICT afdeling altijd nog een backup". De gevolgen van dit onveilige gedrag kunnen groot zijn.

Medewerkers dienen daarom bewust gemaakt te worden van de mogelijke gevolgen van hun handelen.

Staat het onderwerp "security" op de agenda tijdens afdelingsvergaderingen? Vraagt het management input van de afdelingsmanager over de situatie met betrekking tot de security?

De Sebyde security awareness trainingen en de Sebyde Management workshops zijn uitermate geschikt om een gezonde cultuur te scheppen in een organisatie op het gebied van security.

Voor meer informatie over deze training en workshop, lees verder

Vragen die elk bedrijf zou moeten beantwoorden

Om een goede start te maken voor het verlagen van risico's is het goed als een bedrijf eerst eens een inventarisatie maakt. Gewoon eens op papier zetten wat de status is. Om een beetje op weg te komen volgen hier een aantal vragen waarvan elk bedrijf de informatie gedocumenteerd zou moeten hebben.

Het is ook een goede oefening ter voorbereiding op de nieuw aangekondigde privacy wetgeving.

1. Waar staat uw (digitale) informatie?
2. Welke waarde heeft die informatie binnen uw bedrijf?
3. Welke dreigingen zijn er?
4. Wie heeft toegang tot welke informatie?
5. Welke schade kan uw bedrijf oplopen door misbruik of verminking van de data?
6. Hoe groot is de reputatie-schade bij vermelding in de media?
7. Staat security op de agenda van het management en tijdens de afdelingsvergaderingen?
8. Hoe gaan we om met incidenten?
9. Is er een Security Awareness programma?
10. Kunnen de systemen mogelijk de privacy van betrokkenen schaden?

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

Telefoon +31 6 53 23 32 69
Email 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