NIEUWSBRIEF

Sebyde Nieuwsbrief
december 2013 01

In deze **Nieuwsbrief**

Waarom Software laten testen?

Hieronder geven we 5 belangrijke redenen om uw software te (laten) testen op beveiligings-lekken:

Software reparatie is duur

Vroeg testen levert geld op. Het herstellen van een (security) fout in software die al in gebruik is genomen kost 100 keer meer dan het herstellen van die fout als de software nog in ontwikkeling is. Als het lek pas wordt ontdekt wanneer er een incident is geweest zijn de kosten onberekenbaar. Je hebt dan te maken met ongewenste publiciteit, verlies aan klantenvertrouwen en mogelijke schadeclaims.

Software is aan veroudering onderhevig

Had je misschien bij de bouw van een applicatie rekening gehouden met de toen bekende hackmethodes, in de loop van de tijd zijn er steeds nieuwe methodes bij gekomen. Het is verstandig om software periodiek te (laten) testen op die nieuwste hackmethodes, minimaal 2 tot 3 keer per jaar.

Software is complex.

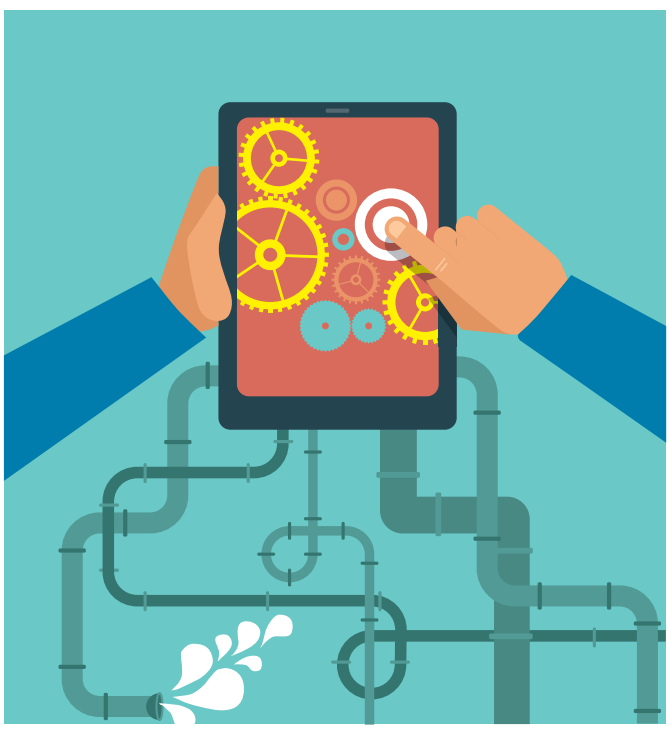
De grote hoeveelheid code in de software van tegenwoordig maakt software een complex product, met vaak zeer specifieke functionaliteit welke geprogrammeerd moest worden. Gedurende de ontwikkeling continue rekening houden met security is dus ook moeilijk en tijdrovend. Voortdurend testen, bijvoorbeeld bij elke iteratie tijdens het ontwikkelproces maakt dat je wijzigingen in verband met security hanteerbaar houd.

Software is overal

Stukken software kunnen overal vandaan komen, bijvoorbeeld via web services. Dus per definitie kan je software niet vertrouwen en moet je deze ook altijd zelf controleren.

Software is duur

De ontwikkeling van software vergt een grote investering. Daarom moet je als leverancier van die software zorgen voor kwalitatief hoogwaardige software. Tevens wil de koper van die software dat de software voldoet aan hoge standaarden en minstens voldoet aan minimale veiligheidseisen. Ook zal de software bijvoorbeeld moeten voldoen aan de wet- en regelgeving voor bijvoorbeeld de privacy en geheimhouding.



Veranderingen in de Privacy wetgeving: Bereid u voor!

De aangekondigde EPV (Europese Privacy Verordening) gaat grote gevolgen hebben op de security maatregelen van organisaties. Er worden concrete maatregelen gevraagd om de privacy van de gegevens te waarborgen. De mogelijke privacy impact van systemen dient gecontroleerd te worden middels een audit, Privacy Impact Assessment (PIA). Nieuwe systemen moeten straks voldoen aan het "Privacy by Design" principe. Met andere woorden: de wetgeving moet in de systemen worden ingebouwd. Torenhoge boetes (2% - 5% van de wereldwijde omzet!) zijn aangekondigd bij non-compliance.

Afgelopen 21 oktober 2013 is de concept wet van de EPV na het doorvoeren van vele aanpassingen bij een stemming van de Europese commissie goedgekeurd. In April/Mei 2014 zal tijdens een plenaire sessie van de Europese commissie over de definitieve wet worden gestemd. Aangezien de stemming op 21 oktober zeer overtuigend was (49 stemmen voor, 3 tegen) is de verwachting dat de nieuwe wet definitief wordt goedgekeurd.

Aangezien het hier om een verordening gaat zal de wet dan ook direct van kracht worden in alle Europese lidstaten.

Een belangrijk aspect is dat er bij de nieuwe wetgeving ook duidelijke verantwoordlijkheden zijn omschreven voor de hosting partijen en aanbieders van Cloud-diensten. Veel bedrijven verschuilen zich nu achter hun hosting partij als het gaat om security maatregelen. "Dat regelen zij wel".
De eindverantwoordelijkheid voor de verwerking van de data ligt echter bij de eigenaar van de gegevens.
Omdat er straks torenhoge boetes uitgedeeld kunnen worden zullen de hosting partijen straks dus verzoeken krijgen van hun klanten om aan te tonen dat hun privacy impact onderzoek is uitgevoerd.

Bedrijven dienen zich nu voor te bereiden op de EPV. Neem contact op met Sebyde BV over de mogelijkheden die er zijn om uw privacy- en Security situatie in kaart te brengen.
Kijk op http://www.sebyde.nl/downloads en download het document over het Sebyde Privacy onderzoek.

Security Awareness Training

Bij het streven van een organisatie om de risico's naar beneden te brengen speelt het al dan niet veilige gedrag van de gebruikers van uw informatiesystemen een belangrijke rol. Iedereen in de organisatie heeft te maken met ICT en informatie, iedereen speelt daarom een belangrijke rol in het proces van het beschermen van de eigendommen van het bedrijf. Gebruikers zijn zich vaak niet echt bewust van de risico's en de dreigingen.

Tijdens de Sebyde Security Awareness training gaan we uitgebreid in op de waarde van de informatie en de risico's en dreigingen die er zijn. We leren de medewerkers hoe ze van onveilig naar veilig gedrag kunnen gaan en de security-aspecten mee laten nemen in hun dagelijkse activiteiten. Dit gaat met behulp van een uitgekiende leermethodiek die de medewerkers in staat stelt om de informatie in hun eigen werkomgeving toe te passen. Dit is een belangrijk element om te voorkomen dat de cursisten na terugkomst van de training weer terugvallen in hun "oude" gedrag.

Ga naar http://www.sebyde.nl/downloads en download het document over de Sebyde trainingen en de leermethode.

Sebyde partner van Stichting Members' Benefits

Sebyde heeft een contract getekend met Stichting Members' Benefits. Daarmee wordt Sebyde de exclusieve partner en leverancier van security-services en security-trainingen.
Stichting Members' Benefits (SMB) is een stichting die is voortgekomen uit de grootste branchevereniging in Nederland, de Federatie voor de Metaal- en Electrotechnische industrie (FME). De stichting onderhoudt diverse voordeelregelingen voor meer dan veertig werkgevers- en brancheverenigingen waar circa 15.000 bedrijven als lid bij zijn aangesloten.
Sebyde gaat een breed scala van diensten aanbieden. Om te beginnen biedt Sebyde Webapplicatie Security Scans om websites te controleren op security-kwetsbaarheden.
Dit is een zeer effectieve service om hackers-aanvallen te kunnen doorstaan.
Verder geeft de organisatie Security Awareness-trainingen om het gedrag van medewerkers veiliger te maken.
Hiermee wordt de kans op cyber-crime binnen organisaties verlaagd. Ook geeft het bedrijf Security Awareness-trainingen voor programmeurs. Hier leren softwareprogrammeurs om veilige software te bouwen die de hacker-aanvallen kunnen doorstaan. Daarnaast organiseert Sebyde managementworkshops. Daarin wordt het deelnemers duidelijk hoe zij een Security Awareness-programma in hun organisatie moeten implementeren door inzicht te geven in de doelen en een praktisch overzicht te maken van de te nemen stappen tijdens dit proces. Sebyde kan deelnemers tijdens de informatiebijeenkomsten over Security Awareness en Privacy meer leren over de gevaren, dreigingen en risico's die het werken met informatiesystemen met zich meebrengen. Ten slotte biedt de organisatie verschillende vormen van security-onderzoek aan zoals een penetratietest, een applicatietest of een Privacy Impact-onderzoek.

Volg ons op: