



Compliance

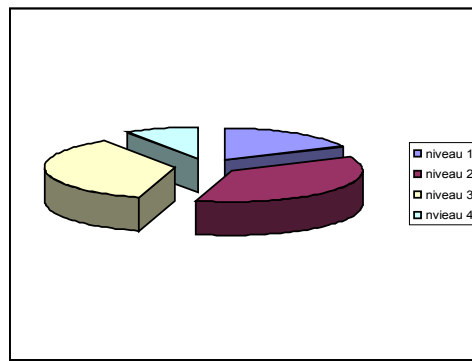
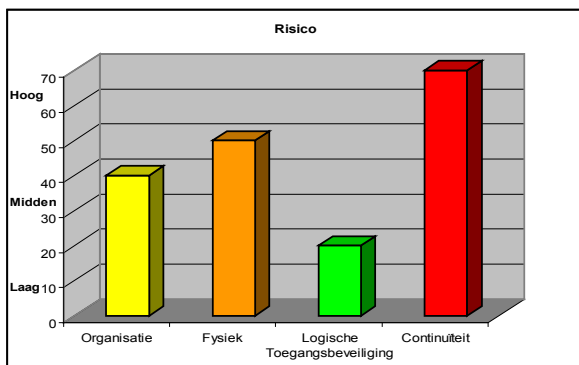
Toenemende regelgeving bij ondermeer banken en verzekeringen heeft ertoe geleid dat compliance met Wet- en Regelgeving een steeds belangrijkere plaats heeft ingenomen binnen organisaties. Voor banken en verzekeringen geldt bijvoorbeeld dat compliant zijn met Basel II van groot belang is. Compliant zijn met Sarbanes Oxley is voor organisaties die genoteerd staan op een Amerikaanse beurs verplicht.

Wat is precies compliance? Compliance wordt omschreven als "de naleving van wet- en regelgeving, alsmede het werken volgens de normen en regels die een instelling zelf heeft opgesteld".

Naast bovengenoemde regelgeving speelt ook informatiebeveiliging een steeds belangrijkere rol. Veel organisaties gebruiken de ISO 17799 als uitgangspunt bij het formuleren van hun eigen beveiligingsrichtlijnen. Het compliant zijn met deze richtlijnen is voor veel organisaties belangrijk.

Het toetsen of en in welke mate een organisatie voldoet aan bepaalde regelgeving kan gebeuren door middel van een regelmatige self assessment en rapportage aan het hoogste management.

Bij het meten of en in welke mate de organisatie voldoet aan een bepaalde richtlijn, worden veelal een aantal niveaus onderscheiden. Dit worden ook wel volwassenheidsniveaus (maturity levels) genoemd. Aan de mate van compliance kunnen conclusies worden getrokken. Bij compliance met de ISO 17799 kan per groep van regels (bijvoorbeeld fysieke beveiliging) worden vastgesteld in welke mate men voldoet en welke risico's worden gelopen.



Essentieel bij het meten van compliance is de rapportage aan het management.

Bovenstaand is een tweetal voorbeelden van rapportage over de mate waarin men compliant is met een (groep van) richtlijnen en wat de consequenties zijn in (beveiligings-)risico's voor de organisatie.

Het management zal behalve een mate van compliance en een rapportage over risico's ook willen weten wat de vooruitgang of achteruitgang is ten opzichte van een vorige rapportage. Op deze manier wordt inzicht verkregen of bijsturing het gewenste effect heeft gehad.

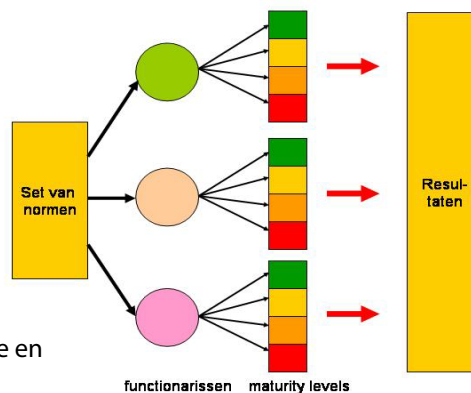
Uitvoering

Bij de uitvoering van de meting is het van belang om eerst vast te stellen welke functionarissen in de organisatie verantwoordelijk zijn voor welke regels. Dit zijn ook de functionarissen die voor hun deel moeten rapporteren in hoeverre de organisatie compliant is.

Hiernaast is afgebeeld hoe een set van normen wordt verdeeld over diverse functionarissen.

Het moge duidelijk zijn dat ICT-ondersteuning bij het meten van compliance een must is.

Secure Connection kan u ondersteunen bij een goede keuze en invoering van een geautomatiseerd programma



Secure Connection heeft client-server infrastructuur voor kennis objecten.

Secure Connection heeft eind vorig jaar een client-server infrastructuur voor kennisobjecten gelanceerd. Hiermee is het mogelijk om onze kennisprogramma's centraal te beheren, terwijl meerdere (groepen van) medewerkers gebruik kunnen maken van de kennisprogramma's en van de resultaten van andere medewerkers. Zo is het bijvoorbeeld mogelijk om een analyse door meerdere mensen uit te laten voeren. Dit biedt veel meer mogelijkheden dan het stand-alone werken met de kennisobjecten.

In de brochure StandardGUI infrastructuur wordt het principe van een infrastructuur voor kennisobjecten en de diverse uitvoeringen beschreven. Deze brochure zal met deze nieuwsbrief aan u worden verzonden.

Actueel

Rootkit worm steelt wachtwoorden

In onze vorige nieuwsbrief was een artikel over rootkits opgenomen. In deze nieuwsbrief is er aandacht voor een nieuwe trojan horse, die gebruik maakt van rootkit technieken.

Sana Security kwam deze week met de mededeling dat zij een rootkit worm hebben ontdekt, die gebruikersnamen en wachtwoorden steelt.

De trojan horse, rootkit.hearse genoemd, gebruikt rootkit technieken om zichzelf te verbergen voor virusscanners.

De rootkit maakt bij het stelen van gebruikersnamen en wachtwoorden geen gebruik van zogenaamde "keystroke" technieken maar komt in actie als een gebruiker een site bezoekt, waarbij een username en een wachtwoord moet worden opgegeven. De username en wachtwoord wordt vervolgens doorge-

stuurd naar een russische site. Deze site is niet beveiligd, waardoor alle user namen en wachtwoorden zijn op te vragen. Inmiddels waren zo'n 40.000 usernames en wachtwoorden verzameld.

Deze rootkit is een voorbeeld van een groeiende trend van het gebruik van rootkit technieken door virussen.

Met het programma rootkit revealer (gratis te downloaden op (

<http://www.sysinternals.com/SecurityUtilities.html>) kunnen twee files worden ontdekt, namelijk zopenssl.dll en zopensld.sys. De dll draait niet als een apart proces en draait zelfs in safe mode.

Inmiddels is de ISP waar de russische site draait op de hoogte gebracht en verzocht de site uit de lucht te halen.

Bron: www.sanasecurity.com