



Nieuwsbrief 12

In deze Nieuwsbrief

- > Sebyde Internet Weerbaarheid programma
- > Tenable SecurityCenter Continuous View™
- > IBM Security AppScan: Veilige software!
- > Tips ter verlaging van risico's

Sebyde Internet Weerbaarheid programma

U wilt toch ook dat alle medewerkers in uw organisatie bewust en veilig omgaan met de beschikbare ICT middelen? Met het Sebyde Internet Weerbaarheid programma brengt u duurzaam veilig gedrag in uw organisatie.

HR managers en IT beheerders vinden in het Sebyde Internet Weerbaarheid programma een praktisch te implementeren methode om duurzaam veilig gedrag te realiseren. Met dit programma creëert u een goede cultuur met gemotiveerde medewerkers en verlaagt u het aantal incidenten waardoor de continuïteit van de ICT dienstverlening gewaarborgd is.

Het Sebyde Internet Weerbaarheid programma bestaat uit 6 modules, elk met een vast tijds kader en resultaat. Er zijn modules voor zowel management als medewerkers. De doorlooptijd van het programma is ongeveer 1 kwartaal met 6 meetings van een halve dag.

Door middel van logische stappen verbetert u de weerbaarheid van de organisatie en staat het onderwerp security bij iedereen op de agenda. De duurzaamheid wordt geborgd door middel van regelmatige refresh sessies. Hierdoor blijven de medewerkers up-to-date en minimaliseert u de kans op mogelijke terugval naar onveilig gedrag.

Het Sebyde Weerbaarheid programma kent klassikale trainingen en workshops bij u in het bedrijf. Het is een krachtig leerproces door interactie tussen de medecursisten. De trainingen en workshops worden georganiseerd door zeer ervaren coaches en security specialisten.

Graag sturen we meer informatie over het programma toe. Neemt u daarvoor gerust contact met ons op!

Vraag [hier](#) meer informatie over het Sebyde Internet Weerbaarheid programma

Tenable SecurityCenter Continuous View™

Tenable, de leverancier van het bekende Nessus vulnerability management systeem, biedt met het product SecurityCenter™ een geïntegreerd management console voor functie-specifieke rapportages en alerts aan meerdere teams – Security, Compliance, Operations en Incident management.

SecurityCenter™ is een zeer geavanceerd netwerk vulnerability management platform. Het combineert de kracht van Nessus® vulnerability scanning met het vervullen van de informatiebehoefte vanuit de verschillende delen van een organisatie. Het verzamelt en analyseert vulnerability informatie, netwerk- en configuratie-informatie om een compleet overzicht te geven over de security, risico's en de compliance status van de gehele organisatie.

SecurityCenter Continuous View™ biedt een continue monitoring van uw gehele netwerk. Groot voordeel van continue monitoring is dat 100% van de devices (incl. Alle mobile devices!) gedurende 100% van de tijd gezien en geanalyseerd worden door middel van patroon herkenning. SecurityCenter Continuous View™ verzamelt, correleert en analyseert event log gegevens over het netwerkverkeer, intrusion detection gegevens, systeem- en applicatie-logs en gedrag van gebruikers binnen het netwerk. Het combineert actieve scanning, passieve netwerk sniffing en event log analyse waardoor het een real-time continue monitoring platform is. SecurityCenter Continuous View™ ondersteunt meer technologieën dan elk ander product op de markt, inclusief operating systemen, netwerk devices, databases, tablets, telefoons, web-servers en embedded systemen.

Klik [hier](#) voor meer informatie over Tenable Nessus of Tenable SecurityCenter.

IBM Security AppScan: Veilige software!

Security incidenten worden vaak veroorzaakt door kwetsbaarheden in de gebruikte applicaties. Het is daarom van belang om de applicaties te controleren. Dit kan gebeuren door middel van een statische controle van de programmacode of door middel van een dynamische controle van in gebruik zijnde software applicaties. IBM Security AppScan is een product wat al sinds jaren door onderzoekbureaus geadviseerd wordt als marktleider voor het scannen van applicaties op kwetsbaarheden.

Bij het controleren van in gebruik zijnde webapplicaties (bijvoorbeeld uw websites, portals, etc.) wordt de applicatie getest op alle bekende hack methoden om in te breken. Het product wordt gevoed door X-Force, het Research & Development center van IBM wat beschikt over de grootste applicatie vulnerability (kwetsbaarheden) database ter wereld.

IBM Security AppScan Standard Edition genereert vervolgens zeer gedetailleerde rapportages over de gevonden kwetsbaarheden. Deze rapportage kan vervolgens als leidraad dienen bij het uitvoeren van de herstel acties om de gevonden kwetsbaarheden te repareren.

Deze scans verlagen uw risico op (digitale) inbraak enorm. Er zitten in heel veel applicaties ernstige lekken waardoor het letterlijk "kinderspel" is om in te breken. Met een licentie van IBM Security AppScan kunt u tegen lage kosten per maand uw applicaties regelmatig testen op security, grote financiële schade voorkomen en uw compliance waarborgen.

Wij vertellen u graag meer over de mogelijkheden. Wellicht wilt u het product eens in werking zien? Bel hiervoor gerust met ons voor het maken van een afspraak.

Vraag [hier](#) meer informatie over IBM Security AppScan.

Tips ter verlaging van risico's

Inventariseer uw data en registreer de incidenten

Als je niet weet wat je hebt, kun je het ook niet beschermen. Maak eens een inventarisatie van de aanwezige gegevensbestanden in uw bedrijf. Registreer deze gegevens. Waar staat het? Wie is de eigenaar? Wie heeft er toegang? Welke informatie betreft het? Waarom is het nodig? Zijn het persoonsgegevens? Toekomstige nieuwe wetgeving gaat dit in ieder geval van u vragen.

Het is sterk aan te raden om alle security incidenten te laten melden bij een centraal contactpersoon. Alleen dan kun je na verloop van tijd een goede inschatting maken van de gevaren en dreigingen waar de organisatie aan bloot staat. De hoeveelheid risico komt in kaart en de juiste maatregelen kunnen genomen worden.

Klik [hier](#) voor meer informatie over ons Privacy onderzoek.



Sebyde

Verlaagt het aantal incidenten door middel van security checks van applicaties, netwerken en systemen.

Verhoogt de weerbaarheid van uw organisatie door trainingen, workshops en presentaties van de Sebyde Academy

Leidt management workshops ter voorbereiding van het implementeren van een Security Awareness programma.

Bepaalt en controleert de privacy status van uw informatiesystemen en organisatie.

U kunt contact opnemen via de volgende links:

Telefoon [+31 6 53 23 32 69](tel:+31653233269)

Email rob.koch@sebyde.nl

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

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

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

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

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