Nieuwsbrief 09

In deze **Nieuwsbrief**

Cyberhygiëne voorkomt aanvallen

In een artikel op de website www.security.nl kwamen we een interessant artikel tegen met de titel "Goede cyberhygiëne kan 80% aanvallen voorkomen". Cyberhygiëne … Wat een prachtig begrip! Het artikel ging over een presentatie van Jane Holl Lute, professor aan het centrum voor Internationale veiligheid en samenwerking aan de Stanford Universiteit.

Het begrip Cyberhygiëne omvat het gedachtengoed dat je als organisatie een aantal maatregelen kunt nemen die veel problemen kunnen voorkomen. Ze benoemt daartoe een aantal belangrijke punten die effectief kunnen helpen om risico's te verlagen. Bijvoorbeeld de inventarisatie van de gebruikte hardware en software. Het is belangrijk om in kaart te brengen wat je hebt. Als je niet weet wat je hebt kun je het ook niet beschermen. Tevens krijg je dan inzicht in de niet geautoriseerde hardware en/of software. Admin-rechten en configuraties van systemen dienen goed gecontroleerd en beheerd te worden. Een goed beleid op dit gebied is noodzakelijk.

Tevens stelt ze dat het belangrijk is om continu assessments uit te voeren naar kwetsbaarheden en ze op te lossen. Kwetsbaarheden kunnen zitten in de hardware en in de software. Pentesten en webapplicaties security (vulnerability) scans halen de kwetsbaarheden boven water. Op deze manier kunt u inschatten welke risico's er zijn en kunt u de juiste maatregelen nemen om de gevonden zwakke plekken in uw beveiliging te repareren.

Uiteraard moeten we ons afvragen welke activiteiten we nog meer kunnen uitvoeren om de risico's te verlagen. Sebyde BV heeft daar goede ideeën over en groepeert deze maatregelen onder de categorieën "Mens", "Processen" en "Techniek".

Graag sturen we meer informatie over hoe Sebyde BV u kan helpen bij het verlagen van risico's. Oftewel het vergroten van uw cyberhygiëne.

Vraag **hier** meer informatie over de Sebyde diensten

Sebyde Academy

Onze Sebyde Academy verzorgt trainingen, workshops en thema presentaties die erop gericht zijn om mensen te stimuleren en motiveren naar veilig gedrag. Een belangrijk aspect binnen het totale spectrum van mogelijke maatregelen die u kunt nemen om de risico's van uw organisatie te verlagen.

In de maanden september, oktober en november zijn er een aantal activiteiten gepland waarvoor u zich via de website van de Sebyde Academy (http://www.sebydeacademy.nl/agenda/) kunt inschrijven. Het zijn effectieve diensten die management en medewerkers bewust maken van de risico's en dreigingen waar we tegenwoordig mee te naken hebben.

Mensen hebben ook updates nodig!
Bij de maatregelen die er genomen worden op het gebied van de security horen natuurlijk de upgrades van de gebruikte software en het patchen van de systemen. Security is nu eenmaal een dynamische wereld. Dagelijks ontstaan er nieuwe bedreigingen die voor organisatie grote gevolgen kan hebben. De mensen die met de ICT middelen werken moeten op de hoogte zijn van de laatste ontwikkelingen met betrekking tot de risico's en de mogelijke gevolgen. Gebruikers zijn een bron van risico als ze niet bewust zijn van de gevolgen en (onbewust) onveilig omgaan met bedrijfsinformatie. De diensten van de Sebyde Academy zijn zodanig ingericht dat ze toepasbaar zijn voor elk bedrijf. Van tweedaagse trainingen, eendaagse workshops of presentatie-sessies van twee uur. Allemaal effectieve diensten die de gebruikers van ICT middelen én hun management bewust maakt. Van alle security incidenten wordt 40% veroorzaakt door menselijk handelen. Sebyde helpt u bij het creëren van de juiste cultuur op het gebied van security en privacy.

Vraag **hier** meer informatie over de trainingen, workshops en thema-presentaties van de Sebyde Academy

Hackers gaan ook naar de tandarts!

In de wachtkamer van de tandarts zag ik pas geleden een aankondiging dat ze voor het gemak van de wachtende patiënten een WIFI in gebruik hadden genomen. De naam van het netwerk was "WIFITandarts" en het wachtwoord was "Tandarts". Een goed bedoelde service natuurlijk. Er zijn nou eenmaal mensen die in de wachtkamer nog even snel hun email willen checken of een whatsapp berichtje de wereld in sturen dat de onvermijdelijke boor nu toch wel erg dichtbij komt. Eenmaal in de stoel gelegen vroeg ik de tandarts of hij zich wel realiseerde dat hackers ook naar de tandarts gaan.

In de vorige editie van deze nieuwsbrief hebben we het aanbieden van een WIFI netwerk al even aangehaald. Nu wil ik hier toch graag wat meer aandacht geven aan de risico's.

Bij het aanbieden van een WIFI netwerk biedt je aan onbekenden Internet toegang aan. Het gebruik van een wachtwoord heeft geen enkel nut als je dat wachtwoord aan de muur van een openbare ruimte ophangt.

Bij het aanbieden van een WIFI zit het gevaar in de mogelijkheid dat het WIFI netwerk door onbevoegden gebruikt gaat worden. Kwaadwillende personen kunnen van buiten af via uw WIFI netwerk ongewenste activiteiten uitvoeren. U wilt daar toch niet aan meewerken?

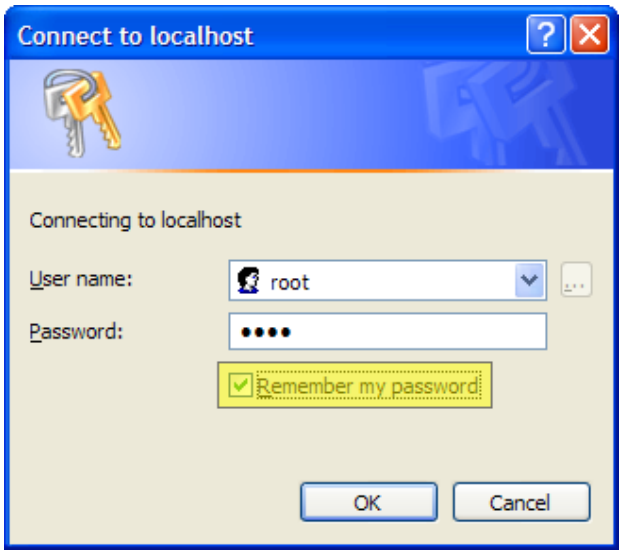
Om de kans op dergelijke situaties te verkleinen dient u ervoor te zorgen dat het WIFI wachtwoord zéér regelmatig wordt aangepast. Schakel tevens buiten de werkuren ('s avonds, weekend) de WIFI router uit zodat het netwerk niet meer toegankelijk is.

Vraag **hier** meer informatie over het gevaar van het gebruik van WIFI netwerken

Tips ter verlaging van risico's

Gebruik geen "Remember my password" functie

Veel programma's bieden de mogelijkheid om je wachtwoord te onthouden. Helaas kun je er niet altijd van uit gaan dat er dan ook security maatregelen zijn ingebouwd om die wachtwoorden ook veilig op te slaan. Sommige programma's slaan die wachtwoorden zelfs onbeschermd in een tekst bestand op. Dit betekent dan dat iedereen die toegang heeft tot de computer ook bij uw wachtwoorden kan komen. Het is echt het beste om wachtwoorden iedere keer bij het inloggen in te typen. Er bestaan handige tools om uw wachtwoorden te beheren, veilig op te slaan en automatisch in te vullen als u inlogt.



Kunnen wij u helpen?

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

Bij het verhogen van het bewustzijn op het gebied van security door trainingen, workshops en thema-presentaties van de Sebyde Academy

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.

U kunt contact opnemen via de volgende links:

Telefoon +31 6 53 23 32 69
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