Beveilig je netwerk tegen computerfraude

Elke tijd kent zijn vorm van criminaliteit. Het is niet verwonderlijk dat in het informaticatijdperk, computerfraude welig tiert. Volgens het gespecialiseerde tijdschrift DataNews werd vorig jaar één op drie bedrijven er het slachtoffer van. De Global Economic Crime Survey van het consultancybedrijf PwC toont computercriminaliteit in de Top 3 van de meest voorkomende fraudetechnieken. Niet alleen een reden, maar een must om er zich tegen te beveiligen.

Een gewone firewall volstaat niet meer om een volledig netwerk te beschermen tegen de gevaren van het internet, zoals hackers of malware. Het gevaar zit immers in een klein hoekje.

Het volstaat dat je een nieuwe (internet) toepassing installeert, onoordeelkundig wijzigingen aanbrengt aan de instellingen van essentiële veiligheidcomponenten of het gebrek aan die componenten, om een organisatie fundamenteel in gevaar brengen.

'De computer' is geen speelgoed meer en de werking ervan is te complex geworden om er op eigen houtje nog veilig mee om te kunnen springen.

Zowel kmo's, grote ondernemingen als overheidsinstellingen zijn het aan zichzelf verplicht, een beroep te doen op gespecialiseerde securitybedrijven om de continuïteit en de goede werking van hun informatica te garanderen.

Zo'n securitybedrijf brengt in eerste fase mogelijke risico's die websites en netwerkinfrastructuur bedreigen, in kaart. Het sterke team van specialisten bestaat uit een mix van application security experts en network security experts. Deze combinatie is nodig om elk project te benaderen volgens de specifieke noden van de klant, op basis van een specifieke vendor- en technologieonafhankelijke methodiek.

Het spreekt voor zich dat je in dit team zelf een blind vertrouwen moet hebben.

Alleen een neutrale expertise kan het antwoord geven op de vraag hoe sterk de internetbeveiliging in feite is.

Er wordt nagegaan waar verbeteringen mogelijk zijn, er wordt gezorgd voor een optimale beveiliging en bovendien wordt erop toegezien dat de geleverde diensten het gewenste resultaat opleveren.

In eerste instantie wordt er een Quick Scan uitgevoerd. Dit is een Health Check die de internetbeveiliging van het bedrijf nagaat. Voor een beperkt budget is al een eerste indruk van de veiligheid van de toepassingen en het netwerk, vast te stellen.

Is er een vermoeden van bedreiging of ontoereikende beveiliging, dan wordt een gedetailleerde Black Box Penetration Test geadviseerd.

Deze test leert of de toegankelijke toepassingen kwetsbaar zijn. De gebruikte methode is gebaseerd op jarenlange ervaring in het manueel testen van webtoepassingen.

Voor elke kwetsbaarheid van het systeem, wordt een rapport opgesteld waarin het probleem duidelijk beschreven staat. De impact en de kritieke elementen worden bepaald en uiteindelijk wordt een plan van aanpak voorgesteld, om het probleem op te lossen, met duidelijke richtlijnen voor de verantwoordelijken.

Bron: Benny De Boeck, www.pjbenedict.be.