Cybercriminaliteit via de website

Er lijkt wel sprake te zijn van een keerpunt in het denken over cyber crime. Steeds meer bedrijven, overheden en organisaties hebben een duidelijk besef dat cyber security niet een 'one-day-fly' is, maar bittere noodzaak. Dit is mede het gevolg van dat bedrijven steeds meer producten en diensten aanbieden via internet; ze moeten wel willen ze niet achterop raken op de concurrentie.

Vaak liggen websites onder vuur als we kijken naar cybercriminaliteit en dus ook data die via een webserver benaderbaar is. Na de werknemer zorgt de webserver voor de grootste security risico's; dit is omdat een webserver een open deur is vanuit een organisatie naar de rest van de wereld.

Belangrijke stappen om dit risico zo klein mogelijk te houden zijn: de server goed te onderhouden, de updates van de web-applicaties op orde hebben en de codering van uw website bepalen uiteindelijk hoe groot uw deur is. Als u uw bedrijf kritische data linkt aan het internet of uw wordt via andere zaken in "zichtbaar" gemaakt dan kunt u er zeker van zijn dat uw web security getest gaat worden.

Op uw website is het voor bezoekers mogelijk gemaakt om:

- een nieuwe pagina te laden met dynamische content;
- zoeken naar een product of dienst;
- invullen contactformulier;
- zoekfunctie op de site;
- mogelijkheden om via web aankopen te doen;
- een account creëren of het inloggen via een bestaand account.

In elk van de bovenstaande gevallen is het voor uw bezoeker mogelijk om een commando via of door uw webserver te versturen en in veel gevallen is dit een database. Een veel voorkomend probleem is dat uw site bestaat uit meerdere programmeer lagen, die door verschillende programmeurs is ontwikkeld en geschreven. Sommige van de codes zijn oud en zijn aangepast of voorzien van nog meer codes door de webdesigner of webmaster. Ook software die jaren geleden is aangeschaft, die misschien niet meer gebruikt wordt en draaiend op verschillende resources zorgen voor grote security risico's en dan vooral door het missen van de belangrijke updates. Elk formulier of script geïnstalleerd op uw site kan zwakheden of zelfs bugs bevatten en zorgen voor beveiligingsproblemen bij u, maar ook bij uw bezoekers. Uw webpagina is namelijk niet het eindstation want dat is vaak uw bezoeker die via uw website wordt besmet.

Het zijn voornamelijk oude beveiligingslekken die cybercriminelen inzetten om exploits te initiëren. Vaak zijn er wel patches uitgebracht, maar het wordt dan vergeten om deze updates te installeren. Hackers maken veel gebruik van deze bekende vulnerabilities omdat betreffende organisaties of websites interessant zijn, maar ook om te kijken of het mogelijk is om ergens in te breken. Ook gezien het feit dat er maar weinig hackers zijn die daadwerkelijk een nieuwe manier vinden om de web security weer te omzeilen.

Ik hoop dat dit artikel u helpt om cybercrime te voorkomen en u de juiste stappen onderneemt om niet gecomprimeerd te worden en dank u voor uw aandacht.