Säkerhetstips

Säkerhetstips Webbhotell/Webbplats

Bör göras - enkelt och bra ...

Det är viktigt att välja **svåra lösenord** och använd inte "admin" som användarnamn någonstans.
Man kommer åt ert utrymme och filer via er webbplats/systems olika scripts (tex Wordpress).
Man kommer även åt allting via cPanel, FTP/SSH och kundarean (Mina Sidor).

Auto Update - Tänk på att uppdatera ert system då säkerhetsuppdateringar följer med varje uppdatering!
Ej uppdaterade Wordpress, Joomla eller andra Open source system är främsta orsaken till intrång el. sabotage.
Det gäller även alla plugins och teman som ligger under ert system, även inaktiva !
Ta bort alla teman/templates och plugins/addons som ni inte använder. Ju fler ni har desto större risk att det finns en exploit (säkerhetshål).

Om ni inte brukar uppdatera er (php) hemsida så stäng av upload funktionen i PHP via PHP väljare i cPanel och options/php valen.
Här kan ni också inaktivera eller ändra andra funktioner i PHP (php.ini/user.ini).
Se till att köra den senaste versionen av PHP som finns tillgänglig i cPanel.

Ta en EGEN backup och spara. Det finns backupfunktion via Autoinstall (Softaculous) hos Wopsa där ni kan sätta upp Auto backups för just den hemsidan.
Sen har ni backup funktionen i cPanel som är enkel att skapa. Se till att ta en fullständig backup då och då OCH LADDA HEM DEN och spara.
Ni kan automatiskt återställa sidan via både autoinstallern och via cPanel med er egna backup.
Wopsas vanliga backuper kan ni också nå via cPanel men det finns en risk att dessa skrivits över beroende på när ni upptäcker skadan.

> Guide till att ta backup finns HÄR.

Mer om ni kan och vill ...

Er config fil för ert system (tex wp-config.php för wordpress) bör inte vara läsbar eller skrivbar för alla!
Ändra till 440 rättigheter (rw.r.0 - via FTP, Shell eller filemanager i cpanel)

Det finns BRA security plugins till de flesta Open source/PHP system (tex wordpress, joomla).
Sök efter - security plugin "wordpress" - under tillägg i ert program eller i en sökmotor.

Läs igenom/sök efter säkerhetstips för just er hemsida.

Flytta mappar och filer utanför er public_html mapp, om det är möjligt och de mappar/filer som ni kan ange egen sökväg till i konfigurationen.

Kör en malware/exploit sökning via någon tjänst på nätet då och då och Virus scanning via er cpanel hos Wopsa.
Sätt upp monitoring på er hemsida så ni får reda på om den är nere eller om något ändrats på en sida som normalt alltid är densamma.

Notering

Wopsa har flera olika säkerhetsprogram som scannar av och stoppar olika hack och intrångsförsök. Det är tusentals per server per dag!
Bruteforce attacker mot FTP/cPanel/SSH/mailkonton - Upload funktioner - Forms - XML - Loginsida - Kodinjektion - Mysqlinjektion - Spammförsök - DDOS olika sätt - Skadlig kod i URL ....
Allt detta och antivirus/malware för filer som laddas upp/skapas och blockering av aktuella kända hacker nätverk, finns uppsatt och fungerar bra hos Wopsa.
Men trots detta är det inte ovanligt att t.ex en Wordpress sajt med ett gammalt tema blir hackat via ett av sina scripts (php filer).

Revision #3
Created 28 December 2022 15:24:48 by WOPSA
Updated 11 January 2023 10:26:41 by WOPSA