Pri ňom som totiž s Dali2 strávil značnú časť dnešného dňa (a včerajšej noci).
Nejaký smrad zahájil hackerský útok na stránky mikroZone (bohužiaľ úspešný) a ako som dnes zistil, nie len na ne.
Čo sa vlastne stalo:

Pri dopísaní poslednej novinky "Ako na datasheety", som zistil že server neodpovedá.
"No čo, výpadok" povedal som si, a pokus o pripojenie opakoval.

Po úspechu som si na mobile našiel SMS od Dali2, že server bol z nejakej príčiny vysoko zahltený, čím nestačil odbavovať požiadavky web stránok.

Po naštartovaní puttyho (remote SSH terminal), som zistil, že nám na serveri pribudli nejaké neznáme súbory, pričom počet spustených perl skriptov sa blížil k číslu 200, traffic na ethernete narastal a mňa začínala bolieť hlava.

Po odstránení nadbytočných súborov a odpálení všetkých neznámych procesov na serveri, som začal hľadať "dieru v plote".
Diera sa čoskoro našla, a problém nastal až pri skúmaní oných nadbytočných súborov.
Vykľuli sa z nich dva regulérne vírusy a jeden podarený script, ktorý nainfikoval všetky dostupné index súbory, čo zapríčinilo ďaľšie rozširovanie vírusu.

Keďže na serveri beži viacero webov, všetky boli "chytené".

A to bola práca na dnes, preto to chvíľku trvalo, kým sme všetko dali do poriadku a zaplátal som dieru v systéme.

Potešilo ma, že po dokončení všetkých prác, sa aj na oficiálnej stránke redakčného systému objavila správa, o tejto bezpečnostnej diere (s krížikom po funuse...)

Takže resultát je momentálne:
Systém je opravený a funkčný. Detaily priebežne dorábam.

**Ospravelňujem sa za výpadok a chýbajúce príspevky.**

p.s. Prečo hackli práve mikroZone? Jednoduché, ľahko nás našli. Odkazy na MZ sú po celom internete.....