Jaký je stav redakčních systémů v doméně .CZ?

Podle statistik Google Analytics se za poslední rok nacházely malware nebo phishing až na 11 procentech otestovaných stránek hostovaných v České republice. Skutečný stav prozkoumali experti z národního týmu CSIRT.CZ.

ZUZANA DURAČINSKÁ

Na časté případy zneužití domény k šíření škodlivého kódu upozorňují kromě Googlu i jiné projekty sdružení CZ.NIC zaměřené na sledování a prevenci škodlivého obsahu v doméně.CZ.

Šíření škodlivého kódu rovněž odhaluje výzkum společnosti Sucuri, ze kterého vyplývá, že ze vzorku 11 000 webových stránek kompromitovaných v roce 2016 bylo 75 procent provozovaných na nějaké verzi CMS. Z těchto 75 procent pak 50 procent na verzi neaktuální.

Pokud někdo provozuje webové stránky na některém z redakčních systémů (CMS), nejjednodušším způsobem obrany je jeho pravidelná aktualizace. Bohužel ne vždy se však tato možnost dostatečně využívá.

V případě, že jsou webové stránky napadené, může se stát hned několik věcí. Uživatelé a zákazníci, kteří se na stránky dostanou, si mohou nakazit své počítače – ti, kteří mají větší štěstí, se tam nedostanou a budou prohlížečem upozorněni, že na dané stránce se nachází škodlivý kód.

Provozovatelé těchto stránek se navíc stanou ve světě internetu nežádoucí.

Pokud nejde o útok zaměřený na konkrétní webovou prezentaci (to se stává hlavně v případech politických stran, vládních stránek a podobně), útoky se většinou uskutečňují automatizovaně bez ohledu na to, zda stránka hostuje e-shop s ponožkami nebo informační stránku zdravotnického zařízení.

Roboti denně procházejí různá metadata webových stránek, z nichž zjišťují verze použitých technologií a ty zranitelné pak často zneužívají.

Národní bezpečnostní tým CSIRT.CZ, který provozuje sdružení CZ.NIC, má mimo jiné za úkol působit také v oblasti prevence. Má tak za sebou například přednášky o doporučené politice hesel, ale také třeba právě upozorňování provozovatelů webových stránek na rizika spojená s provozováním webu se zastaralou verzí redakčního systému.

K aktivnímu vyhledávání zranitelných zařízení dostupných z internetu se tým CSIRT.CZ navíc zavázal ve veřejnoprávní smlouvě, která definuje rozsah činností Národního bezpečnostního týmu.

[Roboti denně procházejí různá metadata webových stránek, z nichž zjišťují verze použitých technologií a ty zranitelné pak často zneužívají.]

Jak probíhalo testování?

Výzkumníci CSIRT.CZ otestovali celou zónu .CZ. Používané verze redakčních systémů se zjišťovaly z HTML hlaviček webových stránek nebo ze známých souborů specifických pro daný systém CMS, které verzi uvádějí.

Experti se zaměřili na nejpoužívanější redakční systémy, kterými jsou WordPress a Joomla. U WordPressu se věnovali pouze verzím 4.7.5 a starším, u Joomly pak verzím starším než 3.7.

Celkem se identifikovalo 50 761 domén .CZ se zastaralou verzí některého z CMS, z nichž bylo 25 606 verzí CMS Joomla a 25 155 verzí WordPressu. Všichni držitelé domén se následně prostřednictvím e-mailu o této skutečnosti informovali.

Graf č. 1: Instance Joomla nižší než 3.7 mezi dny 23. 7.–29. 8.