Skener webov pre mestá a obce

Mgr. Zuzana Duračinská, špecialistka počítačovej bezpečnosti, CZ.NIC, z. s. p. o.

Angažovanie miest a obcí vo virtuálnom priestore sa zvyšuje. Tak ako bol mestský, respektíve obecný web ešte pred pár rokmi raritou a skôr doplnkovou službou obecnej samosprávy, v roku 2014 sme sa posunuli do fáze, kedy sa webová aplikácia stala samozrejmosťou. Ak vezmeme do úvahy históriu miest a obcí, časové obdobie za ktoré sa obecné webové aplikácie vyformovali do dnešnej podoby je nezanedbateľne malé.

V roku 1992 sa uskutočnilo na Českom vysokom učení technickom v Prahe oficiálne pripojenie Českej republiky k počítačovej sieti Internet. V deväťdesiatych rokoch sa Internet postupne rozširoval do súkromného sektora a v roku 2001 bolo podľa Českého štatistického úradu už 5,1 %[1] domácností pripojených na Internet. Rýchly trend pripojenia k Internetu a jeho využívania spôsobil, že v roku 2013 to bolo už 67 %[2] domácností. Na tento trend museli rýchlo reagovať aj mestá a obce a preto okrem zavádzania iných informačno-komunikačných prostriedkov sa začali tvoriť aj obecné weby. Postupne sa tak začali obecné informácie zverejňovať na obecných weboch a miesto komunikácie s občanmi sa presunulo po stáročiach do novej dimenzie v priebehu pár rokov.

V úplných začiatkoch bolo dôležité obecnou webovou prezentáciou disponovať. Nájsť človeka v rámci obecnej organizácie, ktorý by dokázal webovú aplikáciu vytvoriť bolo v minulosti pomerne náročné, pretože iba pomerne malý počet ľudí sa tejto problematike venoval. Dnes sa situácia postupne zlepšuje a v obecnom rozpočte sa nájdu prostriedky aj na odborníka z oblasti IT, prípadne sa táto služba outsourcuje. Napriek tomu, že obce už svojich IT odborníkov majú, často nedokážu naplniť všetky požiadavky, ktoré by dnes mali weby spĺňať.

Obecné prezentácie sa vyvinuli nielen po stránke vizuálnej, ale aj po stránke funkčnej a obsahovej. Kritéria, ktoré by obecný web mal plniť kontinuálne narastajú. Dnes sú na stránky kladené pomerne vysoké požiadavky a jednou z nich je aj ich bezpečnosť. Postupné rozširovanie služieb na obecných weboch však ide ruka v ruke aj so zvýšenými nárokmi na programátorov a bezpečnosť. Občania očakávajú, že pokiaľ vstupujú na stránky obce neprenesú si na svoje zariadenia vírusy a iný škodlivý obsah. Dobre zabezpečený web je vizitkou obce. Často je však náročné, aby jeden pracovník dokázal zabezpečiť širokú funkcionalitu stránok s mnohými službami a zároveň bol schopný vnímať objektívne aj ich zabezpečenie. S týmito novými „povinnosťami“ sa musia obce a mestá postupne stotožniť a vnímať ich ako integrálnu súčasť poskytovania služieb občanov.

Kým sa tak stane, národný bezpečnostný tým CSIRT.CZ sa rozhodol o svoje skúsenosti z bezpečnosti podeliť a od augusta 2013 poskytuje obciam bezplatnú službu Skener webu - https://www.skenerwebu.cz/. Cieľom služby je odhaliť bezpečnostné zraniteľnosti, ktoré sa na weboch nachádzajú a navrhnúť kroky na ich odstránenie. Penetračné testovanie v tomto prípade spočíva v odhaľovaní bezpečnostných chýb, ktoré môže potencionálny útočník využiť vo svoj prospech.

Jeden z dôvodov, prečo sa tým CSIRT.CZ, ktorý operuje pod hlavičkou správcu národnej domény .CZ združenia CZ.NIC, rozhodol poskytovať obciam túto službu vyplýva zo sledovania domén, ktoré sa nachádzajú na tzv. blacklistoch. Pokiaľ sa objaví podozrenie, že stránky obsahujú škodlivý obsah, vyhľadávače ich umiestnia na tieto čierne listiny a zablokujú ich dovtedy, kým sa problém neodstráni. CSIRT.CZ tieto čierne listiny pravidelne sleduje a následne o tom informuje držiteľov domén. Aplikácia k tomu vytvorená sa nazýva Malicious Domain Manager. Vzhľadom však k tomu, že problémy sa často opakujú, sme sa rozhodli doplniť reakčné kroky po nákaze krokmi preventívnymi.

Podľa 10 najčastejších okruhov zraniteľností organizácie OWASP Top 10 sme po spustení služby začali na základe prijatých objednávok testovať okrem iného aj obecné weby. Testovanie prebieha automatickými nástrojmi a ručne. Aj keď automatické nástroje dokážu prechádzať stránkami hodiny a identifikovať zraniteľnosti od tých najľahších cez kritické, ľudský faktor je nevyhnutný na správnu interpretáciu týchto výsledkov a ich doplnenie. Automatizované nástroje nachádzajú okrem reálnych zraniteľností aj tzv.false positive. Tie spočívajú v tom, že nástroj identifikuje ako zraniteľnosť niečo, čo v skutočnosti zraniteľnosť nie je. Pri ručnom teste dokáže tester takisto posúdiť riziko zraniteľností podľa zamerania stránky, prípadne testovanej služby a rozšíriť bezpečnostné testovanie o faktor ľudskej logiky.

[1] http://www.czso.cz/csu/dyngrafy.nsf/graf/cr_od_roku_1989_pc
[2] http://www.czso.cz/csu/redakce.nsf/i/informacni_technologie_pm

Po prvých desiatkach otestovaných webov sme sa presvedčili, že nielen obecné, ale aj komerčné weby majú značné nedostatky v zabezpečení. Až 8% všetkých nájdených zraniteľností na weboch, ktoré sme zatiaľ otestovali sa týkali kritických chýb, ktoré majú na svedomí napríklad zmenu obsahu stránok, obmedzenie práv administrátora stránky či nahratie škodlivého obsahu. Omnoho viac, až cca 26 % zraniteľností nachádzame s vysokým rizikom. Tieto zraniteľnosti sa týkajú hlavne nedostatočnej politiky hesiel, využitia komponentov verejne známych zraniteľností, ktoré vyplývajú z neaktuálnych programov či absencie šifrovaného spojenia pri prihlasovaní sa do administrátorských či užívateľských rozhraní. Napriek tomu, že pred mnohými útokmi je možné sa chrániť základnými doplnkami napríklad v hlavičkách požiadaviek a v cookies, mnoho administrátorov tento fakt opomína. Ide napríklad o obmedzenie vkladania strániek do <framu> či nastaveniu flagu „HTTP Only“ u cookies, ktorý predchádza krádeži cookie. Tieto nálezy potom uvádzame ako informačné s cieľom pomôcť administrátorom rozšíriť celkovú úroveň zabezpečenia webu.

Čas, ktorý sme službe zatiaľ venovali spolu s narastajúcim počtom otestovaných webov nás presvedčil o stále nedostatočnej pozornosti venovanej tejto problematike a opodstatnenosti služby. Každá webová aplikácia, za ktorou stojí človek je iná a špecifická. Preto sa takisto rôznia nachádzané zraniteľnosti, ktoré sa líšia rizikom zneužitia od informačného nálezu po kritický. V prípade kritických nálezov dostáva tester/prípadný útočník pod kontrolu napríklad celý obsah webovej aplikácie. To je možné potom zneužiť na šírenie napríklad škodlivých vírov, falšovania stránok bankových inštitúcií (tzv. phishing) či zmenu obsahu webu so zameraním na poškodenie dobrého mena. V prípade iných útokov môže ísť napríklad o zmenu prihlasovacích mien a hesiel užívateľov.

Keď weby slúžili na jednostranné poskytovanie informácie od obce k občanovi, riziko bolo nižšie. Dnes však obecné stránky poskytujú aj možnosť zdieľania informácií od občana k obci a s ohľadom na citlivosť informácií ako sú napríklad osobné údaje sa otázka zabezpečenia stáva do rovnocennej pozície s funkčnosťou. Pokiaľ sa obce a mestá nestotožnia aj s touto stránkou nielen webových prezentácií, ale aj informačno-komunikačných systémov ako takých, budeme sa snažiť podať im pomocnú ruku.

Vzhľadom k tomu, že z výsledkov testovania vychádzajú pomerne citlivé informácie, dbáme na to, aby žiadatelia boli oprávnený a ako formu autentizácie podávania objednávky príjmame úradne overený podpis a elektronický podpis od akreditovaných certifikačných autorít. Objednávku môže za obec zaslať starosta alebo iná poverená osoba. V prípade akýchkoľvek otázok je možné sa obrátiť na podpora@skenerwebu.cz. Služba bola vyvinutá práve pre neziskový a verejný sektor, preto by obce nemali váhať a túto možnosť využiť.

Obce majú dôležitú úlohu pri zabezpečovaní chodu obce a uspokojovania potrieb občanov. Zároveň však majú pomerne obmedzené prostriedky. Dúfame, že touto službou im uľahčí národný bezpečnostný tým CSIRT.CZ túto neľahkú úlohu. Napriek tomu, že dôveru si môžu obce budovať kontinuálne aj niekoľko desaťročí, pri opomenutí bezpečnosti ju môžu veľmi rýchlo stratiť. Pokiaľ boli všetky informácie uložené na úrade, dvere boli stále zamknuté. Prečo by to však malo byť inak, ak sa informácie presunú do virtuálneho priestor.