BAKI UNİVERSİTETİNİN XƏBƏRLƏRİ
№2 *Fizika-riyaziyyat elmləri seriyası* 2007

WEB-SAYTLARİN TƏHLÜKƏSİZLİYİNİN TƏMİN OLUNMASİ ÜÇÜN BƏZİ TƏDBİRLƏR HAQQİNDA

R.F.FƏRƏCULLAYEV
AMEA İnformasiya Texnologiyaları İnstitutu

Məqalədə web-sistemlərdə informasiya təhlükəsizliyinin aktuallığına diqqət yetirilir, web-saytların təhlükəsizliyinin müxtəlif səviyyələri haqqında və web-sistemlərdə informasiya təhlükəsizliyinin təmin edilməsi üçün mövcud tədbirlər haqqında danışılır. Respublikada son zamanlar baş verən web-sayt hücumları və bu hücumlar nəticəsində sıradan çıxarılmış saytlar bu sahəyə diqqətin daha da artırılmasının, eləcə də növbəti hücumlara qarşı dayanıqlılığın daha da möhkəmləndirilməsinin və təhlükəsizliyin gücləndirilməsinin vacibliyini göstərməkdədir. Bu səbəbdən də web təhlükəsizliyi və onun müxtəlif səviyyələrini daha yaxşı anlamaq və mümkün tədbirləri bilmək vacibdir. Məqalədə həmçinin web təhlükəsizlik haqqında daha ətraflı informasiya toplanması və ən son yeniliklərin əldə edilməsi üçün müxtəlif web istinadlar tövsiyə olunmuşdur.

Web-saytların təhlükəsizliyinin təmin olunması şəbəkə arxitekturasının təhlükəsiz planlaşdırılması və yaradılması ilə başlanır. Şəbəkədə ən çox hücumlara məruz qalan komponentlər web-saytlar və web-serverlərdir [1]. Xüsusilə son zamanlar hakerlərin web-saytlara hücumları çox fəallaşmışdır. Respublikada haker hücumlarına məruz qalmış saytlara AMEA-nın rəsmi www.science.az (www.elm.az) portalını və İctimai Televiziyanın www.itv.az saytını misal göstərmək olar. Bu gün hakerlik o qədər inkişaf etmişdir ki, hətta İnternetdə belə hücumları həyata keçirmək üçün hazır proqram təminatları və məqalələr yer almaqdadır [2].

Web-saytların haker hücumlarına qarşı davamlılığını artırmaq üçün web-serverin dizaynından başlamaq tövsiyə olunur. Web-serverin əməliyyat sisteminin və web-server proqram təminatının düzgün seçilməsi, quraşdırılması və düzgün konfiqurasiya edilməsi çox mühümdür [3]. Daha sonra isə ayrı-ayrı proqram təminatlarının və əməliyyat sisteminin yeni versiyalarının daim nəzarətdə saxlanılması, yeni versiyaların və ya təhlükəsizlik pətçlərinin (patch) quraşdırılması və təhlükəsizliyin dövri olaraq yoxlanılması əsas məsələlərdən biridir.

Serverin əməliyyat sistemi və proqram təminatları quraşdırılandan və konfiqurasiya ediləndən sonra diqqəti web-saytların və web-proqramların təhlükəsizliyinə yönəltmək lazımdır. Şəbəkə əməliyyat sisteminin (ŞƏS) və proqram təminatlarının düzgün sazlanmasına baxmayaraq, serverdə yerləşdiriləcək web-proqramlar yeni təhlükəsizlik boşluqları açа bilər. Belə boşluqlar isə bəzən sadə HTTP sorğusu əsasında həyata keçirilən hücumlara qarşı davamsız olur [4]. Web-saytların yaradılması zamanı skriptlərin təhlükəsiz kodlaşdırılmasına və effektiv

proqramlaşdırma üsullarına riayət etmək vacibdir. Əgər saytın yaradılması zamanı yeni təhlükəsizlik boşluqlarının yaranmaması üçün bu prinsiplərə əməl ediləcəyindən əmin deyilsinizsə, onda web-proqramların/saytların yaradılması üçün outsorsinqdən (outsourcing – kənardan mütəxəssis dəvət etmək) istifadə etmək tövsiyə olunur. Web-saytların professionallar tərəfindən yaradılması özü də təhlükəsizliyin təmin olunması istiqamətində atılmış mühüm addımdır.

Web-serverlərə edilən hücumlar müxtəlif növlü və müxtəlif səviyyəli ola bilər [5]. Təhlükəsizliyin təmin olunması üçün bu səviyyələrin hər birinə ciddi əməl edilməlidir.

1. **Web-serverin fiziki təhlükəsizliyi**. Web-serverin təhlükəsizliyi fiziki səviyyədə elə təmin olunmalıdır ki, istənilən şəxsin web-serverin arxasında əyləşib ona istədiyi müdaxilələri etməsi mümkün olmasın. Bunun üçün web-serverin yerləşdiyi otaqlar xüsusi mühafizə vasitələri ilə qorunur. Güclü parollar təyin edilir və parollar məxfi saxlanılır.
2. **Web-serverin texniki təhlükəsizliyi**. Bu səviyyəyə şəbəkənin düzgün strukturlaşdırılması, şəbəkənin təhlükəsizliyinin təmin olunması üçün istifadə olunan avadanlıqların və web-serverin sistem resurslarının seçilməsi nəzərdə tutulur. Burada CİSCO və Juniper kimi şirkətlərin təhlükəsizliyinin təmin olunması üçün təklif etdiyi qurğuların (Load Balancers, Routers, Firewalls, Proxies, etc.) tətbiq olunması tövsiyə olunur. Texniki səviyyəyə verilənlər bazası serverinin, web-serverin və digər komponentlərin şəbəkədə yerləşdirilməsi də daxildir.
3. **Proqram təminatı təhlükəsizliyi**. Web-serverin təhlükəsizliyi həmçinin onun istifadə etdiyi əməliyyat sistemindən və orada yüklənmiş proqram təminatından da asılıdır. Web-server üçün təhlükəsiz fəaliyyət göstərə bilən şəbəkə əməliyyat sistemi seçilməlidir. Bundan başqa, web-serverin əməliyyat sistemi və həmçinin həmin əməliyyat sisteminin bütün xidmətləri heç bir təhlükəsizlik boşluqları buraxılmadan sazlanmalıdır. Zaman-zaman bu və ya digər şəbəkə əməliyyat sistemlərinin təhlükəsizlik boşluqları aşkar edilir. Amma çox çəkmədən həmin təhlükəsizlik boşluqlarının aradan qaldırılması üçün xüsusi yeniləşdirmə proqramları (patch) hazırlanır.
4. **Web-saytların təhlükəsizliyi**. Web-serverin təhlükəsizliyinin sonuncu – üçüncü səviyyəsi isə web-serverdə yerləşdiriləcək web-proqramların təhlükəsizliyidir. Ən böyük təhlükə mənbəyi də elə web-serverdə yerləşdirilən web-proqramlardır. Çünki web-serverin fiziki və texniki təhlükəsizliyinin nə qədər yüksək olmasına baxmayaraq, həmin serverdə yerləşdiriləcək web-proqramların açacağı təhlükəsizlik boşluqlarını əvvəlcədən demək mümkün deyil.

Eyni web-serverdə yerləşdirilmiş bir web-proqramı kompromisə gətirməklə həmin serverdəki digər web-proqramlara və ya digər resurslara müraciət etmək mümkündür. Bunların qarşısını almaq üçün web-proqramlar effektiv strukturlaşdırılmalı, web-proqramlara müraciətlər monitor olunmalı, autentifikasiya üçün daha təhlükəsiz metodlar işlənməli, saytlara edilən müraciətlər audit (loq faylların analiz edilməsi) olunmalıdır.

Web-serverin fiziki təhlükəsizliyi

Yuxarıda qeyd edildiyi kimi, web-server təhlükəsiz yerdə yerləşdirilməli və hər cür fiziki təhlükələrdən mühafizə olunmalıdır. Server otağına yalnız müəyyən personalın – administratorların daxil olmasına icazə verilməlidir. Serverlərin daimi elektrik təchizatı və server otağının temperaturu da fiziki təhlükəsizlik səviyyəsinə daxildir. Təhlükəsizlik məsələlərində fiziki səviyyəyə az diqqət yetirilməsi zamanı hətta server otağından avadanlıqların və ya resursların (məsələn, web-serverin əməli yaddaşının – RAM) itməsi və ya dəyişdirilməsi halları baş verir.

Web-serverin fiziki təhlükəsizliyinə, həmçinin güclü parolların təyin olunması və onların məxfi saxlanması, ağızdan-ağıza ötürülməməsi daxildir. Çox zaman hakerlər sistemə daxil olmaq üçün standart parollardan istifadə edirlər. Belə hücumlara lüğət hücumları və ya brut fors (dictionary attacks, brute force) hücumları deyilir. Buna görə güclü parolların təyin edilməsinə xüsusilə diqqət yetirilməlidir [6]. Güclü parol dedikdə sətrinin uzunluğu 6-8 simvoldan az olmayan, tərkibində böyük və kiçik latın hərfləri olan rəqəmlər və xüsusi simvollar (-=[]\;',./~`!@#$%^&*()_+|:<>?) sətri nəzərdə tutulur.

Güclü parolların təyin olunmasından başqa onlar vaxtaşırı dəyişilməli, məxfi saxlanmalı, müxtəlif istifadəçi qrupları üçün müxtəlif parollar təyin olunmalıdır.

Təyin olunmuş parolun güclü olmasını yoxlayan, həmçinin onların oğurlanması üçün hazır proqram təminatları var. Belə proqram təminatlarına "L0phtcrack" proqramını misal göstərmək olar. Bu proqramı www.securitysoftwaretech.com ünvanından əldə etmək olar.

Web-serverin texniki təhlükəsizliyi

Web-serverin texniki təhlükəsizliyi dedikdə ilk öncə serverin sistem resursları nəzərdə tutulur. Web-serverin sistem göstəriciləri zəif olduğu təqdirdə o, DoS və DDoS hücumlarına qarşı davamsız olur. Verilənlər bazasının web-server ilə eyni maşında yerləşdirilməsi texniki cəhətdən zəif planlaşdırmanın əlamətidir. Təhlükəsizliyin təmin olunması üçün müəyyən hallarda web-server ilə VBS (Verilənlər Bazası Serveri) arasında SSL/IPSec kimi təhlükəsizlik protokollarının tətbiq olunması tələb edilir.

Web-serverin təhlükəsizliyinin artırılması üçün müxtəlif şirkətlərin təqdim etdiyi avadanlıqların – load balanserlərin, fayrvolların, proksi və ruterlərin tətbiq olunması mühüm addımlardandır [7].

CİSCO şirkətinin LocalDirector məhsulu sorğuların balanslaşdırılması yolu ilə web-serverin təhlükəsizliyini artırmağa kömək edir. CİSCO Local Director OSİ-nin 4-cü səviyyəsindən (nəqliyyat səviyyəsi) istifadə edərək eyni bir URL-da və eyni bir İP ünvanında bir neçə serverin işləməsini və sorğuların müxtəlif web-serverlərə yönləndirilməsi yolu ilə web-saytların xidmətdən imtina hallarına qarşı davamlılığını artırır. CİSCO LocalDirector 416 saniyədə 7000 sorğuya, CİSCO LocalDirector 430 isə 30000 sorğuya cavab vermək üçün hesablanmışdır. Bu qurğular xidmətdən imtina hallarına qarşı Catalyst 6000 seriyasından olan sviçlər ilə birgə istifadə olunduqda trafiki saniyədə 15 milyon paketə (mpps – million packet per second) qədər sürətləndirmək imkanı verir. LocalDirectorun "synguard" xidməti isə DOS qəbilindən olan SYN hücumlarına qarşı qorunmağa da imkan verir.

Təhlükəsizliyin təmin olunması üçün CİSCO Content Services Switch qurğularından da istifadə edilə bilər. Bu qurğular LocalDirectordan fərqli olaraq content switch funksiyasını da yerinə yetirir. Qərar qəbul etmək üçün burada OSİ-nin 4-7 səviyyələrindən, İP ünvanlardan və s. istifadə olunur. ArrowPoint Content Smart Switch tanınan bu qurğuların CSS 11800 seriyası 20Gbps trafikə nəzarət etməyə imkan verir.

Proqram təminatı təhlükəsizliyi

Burada ilk növbədə web-serverin əməliyyat sisteminin seçilməsi nəzərdə tutulur. Mövcud əməliyyat sistemləri arasında FreeBSD, Unix, Linux, Windows 2003 və s. ŞƏS-dən biri seçilə bilər. Digər proqram təminatlarının seçimi isə ŞƏS seçimindən asılıdır.

ŞƏS-in seçimindən sonrakı mərhələ web-server proqram təminatının və VBİS-in seçilməsi, yüklənməsi və düzgün sazlanmasıdır. Mövcud web-server proqram təminatlarına misal olaraq AOLServer-İ, Apache Web-serveri, İBM HTTP Serveri, MS İİS-i və s. misal göstərmək olar. Bu web-serverlərdən Apache web-serveri Unix əsaslı əməliyyat sistemləri üçün, İİS isə Windows NT əsaslı web-serverlər üçün tövsiyə olunur.

Zaman-zaman ŞƏS-lərin və server proqram təminatlarının müxtəlif yeniləşdirmə proqramları – pətçlər (patch) İnternetdə yerləşdirilir. Pətçlərin serverə tətbiq olunmasında əvvəlcə onların oxşar mühitdə yoxlanması tövsiyə olunur. Ola bilər ki, pətçlərin quraşdırılması prosesi sona qədər davam etməsin və serverə zərər versin. Eyni zamanda bu pətçlər haqqında hakerlərin də xəbərinin olduğunu yaddan çıxarmaq lazım deyil. Təhlükəsizlik qrupunun yeni pətçi yoxladığı vaxt ərzində həmin təhlükəsizlik boşluğu haqqında xəbəri olan haker artıq webserverə hücumlar təşkil edə bilər.

Web-serverin Loq faylları vaxtaşırı analiz edilməlidir. Bundan başqa antivirus və digər proqram təminatları vasitəsilə paket səviyyəli hücumlara qarşı dayanıqlılıq artırılmalı və İDS sistemləri ilə sistemə müdaxilələrin qarşısı alınmalıdır.

Web-saytların təhlükəsizliyi

Təhlükəsizliyin sonuncu səviyyəsi isə web-saytların təhlükəsizliyidir. Burada artıq web-proqramların öz təhlükəsizliyi və HTTP sorğulara qarşı dayanıqlılığı nəzərdə tutulur [8]. Yuxarıda sadalandığı kimi təhlükəsizliyin digər səviyyələrində hücumların qarşısını almaq üçün artıq bir çox proqram və aparat təminatları hazırdır. Buna görə son zamanlar hakerlər web-saytlara hücum edərkən HTTP sorğularından daha çox istifadə edirlər. Belə sorğular proqramçı tərəfindən web-proqramlarda buraxılmış təhlükəsizlik boşluqlarından istifadə edirlər. Hakerlər hücumları təşkil etməzdən əvvəl saytları bir müddət araşdırır, hücumu təşkil etmək üçün hətta lazım gələrsə xüsusi proqram təminatlarını da yaratdıqdan sonra qısa bir müddət ərzində hücumu təşkil edirlər. Belə hücumlara misal olaraq SQL və kod inyeksiyası hücumlarını, sorğu sətrinin və post parametrlərinin dəyişdirilməsi, autentifikasiya informasiyası hücumlarını, XSS hücumlarını və s. misal göstərmək olar. Web-serverdə yeni web-saytlar yerləşdirdikdə orada istifadəçilər tərəfindən nə kimi təhlükəsizlik boşluqlarının araşdırılması tövsiyə olunur. Hazırda İnternetdə HTTP sorğuları əsasında web-saytların təhlükəsizlik boş-

luqlarını araşdıran və əldə edilmiş informasiya əsasında belə hücumları təşkil edən xüsusi proqram təminatları vardır. Belə proqram təminatlarına misal olaraq Burp Suite proqramını (http://www.portswigger.net) misal göstərmək olar. Burp suite proqramı bir proksi proqramı kimi trafik üzərində yerləşdirilir və web-serverə gəlib-gedən bütün trafiki analiz edir. İstənilən an sorğunu və ya web-serverin cavabını dəyişmək imkanı verən bu proqram web-serverin və web-proqramın təhlükəsizlik boşluqlarının araşdırılması və web-serverə növbənöv hücumlar təşkil etmək üçün əvəzedilməz alətdir.

İnternetdə digər növ hücumları təşkil edən və ya web-saytların təhlükəsizlik boşluqlarını analiz edən hazır proqram məhsulları dərc olunmuşdur. Bu tip proqramlar boşluq skanerləri (vulnerability scanner) adı ilə tanınır. Web-saytların İnternetə buraxılmasından əvvəl onların lokal kompüterdə bu cür proqram təminatları ilə sınaqlardan keçirilməsi tövsiyə olunur.

Web-saytların təhlükəsizliyini təmin etmək üçün web-serverin lazımsız xidmətlərinin söndürülməsi tövsiyə olunur. Bununla Amplification attack, Flood attack və s. adları ilə tanınan DoS qəbildən olan hücumların qarşısını almaq olar.

Digər tədbirlər

Təşkilatın web-saytlarının təhlükəsizliyinin təmin olunması üçün xüsusi bir komanda yaradılması tövsiyə olunur. Bu komanda öz təşkilatının web-saytlarının təhlükəsizliyini təmin etməklə yanaşı daima onun daha da təhlükəsiz olması üçün araşdırmalar aparmalı, təhlükələri hamıdan əvvəl aşkar etməklə onları aradan qaldırmağa çalışmalıdır.

Təhlükəsizliyi təmin etmək məqsədilə şəbəkənin bir çox imkanlarını ləğv etmək və bununla da təşkilatın daxilində İnternet istifadəçilərinin narazılığına səbəb olmaq, daxili hücumların meydana çıxmasına və yeni təhlükəsizlik boşluqlarının meydana gəlməsinə səbəb ola bilər. Belə ki, ləğv edilmiş xidmətlərin əvəz edilməsi üçün təşkilatın İnternet istifadəçiləri İnternetdən xüsusi pirat proqram təminatları (Warez) köçürə bilərlər ki, bu da şəbəkə daxilində çoxsaylı virusların, troyanların və casus proqramlarının (Spyware) yayılmasına səbəb ola bilər. Bu isə öz növbəsində təşkilatdan informasiya sızmasına və ya digər təhlükələrə yol açа bilər.

Bu səbəbdən də, təhlükəsizliyin təmin olunması üçün kollektiv yanaşma tələb olunur. Təşkilatın işçilərinin də təhlükəsizlik prinsipləri barəsində savadlandırılması tələb olunur.

Təhlükəsizlik haqqında ən yeni məlumatlar

Təhlükəsizlik çox geniş və çox dərin bir sahədir. Təhlükəsizliyin təmin olunması üçün bir çox əsasların dərindən öyrənilməsi və informasiya təhlükəsizliyi haqqında bir çox məlumatlara malik olmaq lazımdır. Belə məlumatları vaxtaşırı olaraq bu saytlardan almaq olar:

www.securityfocus.com - Əsas təhlükəsizlik xəbərləri saytı. Bundan başqa saytda aşkar edilmiş yeni təhlükələr haqqında xəbərlərə elektron poçt vasitəsilə abunə olmaq imkanı var.

www.securityportal.com – Təhlükəsizlik məsələləri haqqında daha bir güclü sayt. Bu saytda, həmçinin təhlükəsizlik sahəsinə və hakerliyə yeni baş vuran mütəxəssislər üçün yaxşı məqalələr var.

www.atstake.com/security_news - Hakerlər nöqteyi-nəzərindən təhlükəsizlik xəbərləri

http://phrack.infonexus.com – Tarix boyu baş vermiş hakerlik hadisələri və hakerlər haqqında ətraflı məlumat.

www.defcon.org – İl ərzində hakerlərin ən böyük toplantısı Las Veqasda baş verir. Bu saytda hakerlər ilə real əlaqə yaratmat və toplantıları haqqında ətraflı informasiya əldə etmək olar.

www.packetstorm.security.com – Haker proqram təminatları və hakerlik metodları haqqında ətraflı informasiyaya malik bir saytdır.

ƏDƏBİYYAT

1. D.Cameron, “Security İssues for the İnternet and the World Wide Web”, Computer Technology Research Corp., Charleston, South Carolina U. S. A., 1997.
2. R. Gold, "HTTPUnit 1.6 APİ", http://httpunit.sourceforge.net/doc/api/. Jan.10, 2005.
3. Hack Proofing Your E-Commerce Site. Ryan Russell, Teri Bidwell, Oliver Steudler, Robin Walshaw, L. Brent Huston. Syngress 2001.
4. K-OTiK Security, "K-OTik Security Advisories -phpMyAdmin Cross Site Scripting and File İnclusion Vulnerabilities", http://www.kotik.com/english/advisories/2005/0204 accessed Mar.14, 2005.
5. Network Security Bible. Dr. Eric Cole, Dr. Ronald Krutz, and James W. Conley. Wiley Publishing, İnc. 2005.
6. Applied Cryptography and Network Security. Strengthening Password-Based Authentication Protocols Against Online Dictionary Attacks. Springer Berlin / Heidelberg © 2005. İSBN: 0302-9743.
7. W. Cheswick, and S. Bellovin, 1994, “Firewalls and İnternet Security”, Addison-Wesley, Reading, MA, 1994.
8. B. Atkinson, G. Della-Libera, S. Hada, M. Hondo, and P. Hallam-Baker, "Specification: Web Services Security (WSSecurity)," vol. http://www-106.ibm.com/ developerworks/ library/ws-secure/, May 24, 2004.

ВОЗМОЖНЫЕ МЕРЫ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ВЕБ САЙТОВ

Р.Ф.ФАРАДЖУЛЛАЕВ

РЕЗЮМЕ

В статье обращено особое внимание актуальности информационной безопасности в веб системах, рассматриваются различные уровни безопасности и возможные меры для обеспечения информационной безопасности в веб системах. Атаки на веб сайты, произведенные недавно в республике, и сами сайты, разрушенные в результате этих атак, показывают важность оказания большего внимания этой сфере, в том числе укреплению устойчивости и усилению безопасности против будущих атак. Поэтому важно хорошо понять веб безопасность, его различные уровни и возможные меры для его обеспечения. В статье также рекомендуются несколько веб ссылок для получения информации и новостей, связанных с веб безопасностью.

ABOUT A FEW METHODS TO PROVİDE SECURİTY OF WEB SİTES

R. F. FARADJULLAYEV

SUMMARY

İn this article special attention is paid to the topicality of information security on web systems, also spoĸen about several levels of security in web systems and about available measures to provide information security on web systems. Attacĸs made on to sites recently in the Republic and the sites themselves corrupted as a result of those attacĸs are showing the importance paying huge attention in this field, improving robustness and strengthening security against possible attacĸs in future. That is why it is important to deeply understand web security and its different levels, also have ĸnowledge on available measures to provide them. Also, several web linĸs for gathering more information and recent news on web security is supplied with this article.