# Napadnuteľnosť webových aplikácií

**Článok je zameraný na praktické otázky a postupy pri identifikácii bezpečnostných hrozieb webových aplikácií. Uvádza odporúčané spôsoby obrany a protiopatrenia proti týmto hrozbám. Podrobnejšie sa rozoberá metodika organizácie OWASP vo forme desiatich bezpečnostných nedostatkov, na ktoré sa viaže najviac úspešných útokov cez internet. Podobne je uvedená aj metodika inštitútu SANS, ktorá je tiež členená ako desatoro, ale zvlášť pre prostredie Windows a zvlášť pre Linux. Na záver je stručne charakterizované zameranie organizácie US-CERT s odkazom na jej databázu poznatkov a odporúčaní.**

## Úvod

Začiatok nášho storočia sa často označuje ako digitálne desaťročie. Jeho charakteristické znaky sú internetová platforma, softvér ako služba, inteligentné digitálne zariadenia, všetko je založené na XML technológii a nové skúsenosti používateľa. Cieľom je sprístupniť informácie používateľovi kdekoľvek, kedykoľvek a na akomkoľvek zariadení. Bill Gates hovorí: *„V digitálnom desaťročí už nebudeme osobný počítač považovať za nástroj, pomocou ktorého len vykonávame nejaké úlohy. Stane sa pomocníkom, na ktorého sa budeme spoliehať trvalo. Možnosti osobného počítača sa stanú všadeprítomné a spoľahlivo dostupné ako elektrina a zároveň oveľa užitočnejšie ako hocijaké iné zariadenie, ktoré dnes poznáme.“* Imperatívom sa stáva informačné a komunikačné prostredie, zabezpečujúce adaptibilitu, bezpečnosť, spoľahlivosť a škálovateľnosť digitálneho podnikania. Otázka bezpečnosti vo všetkých jej aspektoch sa dostáva na popredné miesto [5], prechádza prudkým vývojom, ktorý má svoj odraz aj v oblasti noriem, štandardov [10] a odporúčaní. Medzi vedúce organizácie v tomto smere patrí OWASP, SANS a CERT. Bezpečnostné iniciatívy konzorcia W3C sú zamerané predovšetkým na XML podpisy a aktivity spojené s protokolom HTTP/1.1 a elektronickým obchodovaním [13].

## Vulnerability

Anglické slovo vulnerability je latinského pôvodu; je odvodené od slov vulnus (rana, zranenie, poranenie; poškodenie, trhlina, diera; úraz, škoda, pohroma, strata; duševná rana, trýzeň, bolesť; hnev, žiarlivosť, láska; úder, bodnutie, pohryznutie; zbraň, strela, šíp), vulnero (raniť, poraniť; ublížiť, uraziť). V angličtine sa termín vulnerable vysvetľuje ako náchylnosť na fyzické poškodenie, na útok, subjekt kritiky alebo výčitky, podliehajúci zvádzaniu alebo presviedčaniu, byť v pozícii prijímania veľkých pokút alebo odmien. V slovenčine nájdeme tiež niekoľko významov – zraniteľnosť, bezbrannosť, napadnuteľnosť, citlivosť, vystavenosť, prístupnosť, exponovanosť, nechránenosť, náchylnosť k poruchám. Z kontextu ešte vyplývajú ďalšie možnosti vyjadrenia termínu vulnerability – slabina, hrozba, ohrozenie, nezabezpečenosť, bezpečnostný nedostatok, ktoré sa používajú ďalej.

## Metodika OWASP

Skupina OWASP (Open Web Application Security Project) sa zameriava na pomoc pri identifikácii bezpečnostných hrozieb webových aplikácií. Vydáva špecifikáciu hrozieb a spôsobov obrany proti nim, ktorej posledná verzia je z r. 2004 [8]. Špecifikácia má tvar zoznamu desiatich bezpečnostných nedostatkov, na ktoré sa viaže najviac úspešných útokov cez internet.

### 1. Neoverený vstup – unvalidated input

Webové aplikácie využívajú vstup z HTTP požiadaviek (občas aj zo súborov) na určenie spôsobu odpovede. Ak informácie z týchto požiadaviek nie sú overované (validované) pred ich použitím vo webovej aplikácii, útočníci môžu sfalšovať hociktorú časť požiadavky HTTP (napr. URL, vyhľadávací reťazec alebo hlavičku), a obísť tak zabezpečovací mechanizmus aplikácie. Validácia parametrov zahŕňa údajové typy, prípustné množiny znakov, minimálnu a maximálnu dĺžku, numerický rozsah, či je povolená nula, či je parameter povinný, prípustné hodnoty (vymenované – enumerácia) a špecifický vzor parametra (regulárny výraz).

### 2. Narušenie kontroly prístupu – broken access control

Kontrola prístupu – tiež známa ako autorizácia – udáva, ako webová aplikácia povoľuje prístup k jej obsahu a funkciám. Ak je nedostatočne zaistená, jej odhalením môžu útočníci získať prístup k účtom, súborom aj funkciám, a teda ich čítať, meniť, mazať či dokonca prevziať ich administráciu. Medzi protiopatrenia možno zaradiť „nepreskočiteľnosť“ nejakých kontrol pred vlastným prístupom a nastavenie vhodných prístupových práv k súborom pomocou mechanizmov operačného systému (väčšina adresárov nemá byť ani čitateľná a čo najmenej súborov má byť vykonateľných). Tiež je vhodné (pomocou HTTP hlavičiek či metaelementov) zabrániť kešovaniu (rýchla pamäť) stránok s citlivými informáciami v prehliadači používateľa.

### 3. Porušenie správy účtov a relácií – broken account and session management

Nedostatočne chránené údaje o účtoch a reláciách (session tokens – prihlasovacie informácie) môžu umožniť útočníkom odmaskovanie a získanie hesiel, kľúčov, session cookies alebo iných tokenov, a tak obísť obmedzenia autentifikácie a dokonca prijať identitu iných používateľov. Bežne používané elementy autentifikácie (login a heslo) je vhodné nahradiť silnejšími metódami autentifikácie (softvérové a hardvérové šifrované tokeny, biometria), ktoré sú však nákladnejšie. Medzi vhodné opatrenia patrí silné heslo (obmedzenie na dĺžku, znaky), periodická zmena hesla, povolený počet opakovaní hesla, kontrola zmeny hesla používateľom, ukladanie hesla v hešovanom alebo šifrovanom tvare, ochrana hesla aj session pri prenose (niečo ako SSL), prenos autentifikačných údajov vždy iba pomocou metódy Post (nikdy nie Get).

### 4. Zneužitie servera na odosielanie skriptov – cross-side scripting (XSS)

Webová aplikácia môže byť zneužitá ako mechanizmus prenosu útoku na prehliadač koncového používateľa. Takýto útok môže odhaliť session token koncového používateľa a napadnúť lokálny počítač alebo sfalšovaním obsahu napáliť používateľa. XSS útok je realizovaný obvykle formou vloženého JavaScriptu, ale potenciálne nebezpečný je každý aktívny obsah (ActiveX, VBscript, Shockwave, Flash atď.). Medzi vhodné protiopatrenia patrí dôsledná kontrola a validácia všetkých vstupných parametrov aplikácie (hlavičiek, cookies, skrytých aj vstupných polí formulárov) vzhľadom na prípustné množiny ich hodnôt. Účinným opatrením je tiež odmietnutie akýchkoľvek HTTP požiadaviek obsahujúcich kód (znaky <, >).

### 5. Pretečenie bufera – buffer overflow

Komponenty webových aplikácií v niektorých jazykoch, ktoré nedostatočne overujú vstupy, môžu byť narušené a niekedy dokonca zneužité na prevzatie kontroly nad procesom. Takými komponentmi sú knižnice, CGI, ovládače aj serverové komponenty webových aplikácií. Odoslaním starostlivo pripraveného vstupu webovej aplikácii môže útočník donútiť túto aplikáciu vykonať ľubovoľný kód. Takýto útok je veľmi ťažké odhaliť a pritom je frekvencia útokov tohto typu vysoká. Citlivými na tieto útoky sú takmer všetky webové servery, aplikačné servery aj prostredia webových aplikácií s výnimkou Java a J2EE prostredí, ktoré sú voči tomuto typu útoku imúnne. Medzi vhodné protiopatrenia patrí pravidelná aktualizácia webových, aplikačných serverov aj iných produktov v rámci internetovej infraštruktúry, ako aj používanie dostupných vyhľadávačov pretečenia bufera. Ďalším opatrením je dôsledná kontrola veľkosti všetkých vstupov aplikácie, prenášaných od používateľa cez HTTP požiadavky. Tiež je vhodné vylúčiť prítomnosť binárnych znakov vo formulároch a následne aj v požiadavkách.

### 6. Vloženie príkazov – command injection

Webové aplikácie pri prístupe k externým systémom alebo lokálnemu operačnému systému prenášajú parametre. Ak sa do takého parametra podarí útočníkovi vložiť škodlivý kód, môže ho externý systém vykonať akoby z poverenia webovej aplikácie. Útokom môže byť volanie operačného systému, volanie externého programu pomocou príkazu shell alebo volanie databázy pomocou SQL príkazu. Útočný skript napísaný v Perle, Pythone či inom jazyku môže byť injektovaný do webovej aplikácie so zlým dizajnom a potom vykonaný. Obsahom skriptu môžu byť špeciálne (meta) znaky, škodlivé príkazy alebo modifikátory príkazov. Zvlášť nebezpečné môže byť prenesenie SQL príkazu, ktoré môže spôsobiť čiastočné poškodenie, porušenie alebo dokonca zničenie obsahu databázy. Protiopatrenia – v prvom rade dôsledná kontrola vstupov, tri úrovne blokovania pomocou firewallovej technológie – vysoká (úvodzovky), stredná (úvodzovky plus príkazy OS) a nízka (zamietnutie príkazov OS), zamedzenie volania externých zdrojov (system, exec, fork, Runtime.exec, SQL queries alebo čokoľvek, čo vytvára syntax požiadavky na interpreter). Ďalším opatrením je organizovať činnosť webovej aplikácie len s minimálnymi, nevyhnutne potrebnými právami (teda nie root pre webový server alebo dbadmin pre databázu). V prípade nutnosti použitia externého príkazu sa musí informácia vkladať do príkazu čo najprísnejšie a čo najpresnejšie kontrolovať.

### 7. Nekorektné spracovanie chyby – improper error handling

Spracovanie chybových situácií a podmienok webovej aplikácie nie je stopercentne vyriešené a ošetrené. Ak sa podarí útočníkovi vyvolať takú chybovú situáciu, ktorá nie je webovou aplikáciou ošetrovaná, môže získať celý rad detailných systémových informácií aj prehľad o produktoch a technológiách danej inštalácie. Na ich základe môže zostaviť tzv. exploit – program na zneužitie slabých miest a ním spôsobiť odmietnutie služby či vyradenie bezpečnostného mechanizmu webovej aplikácie alebo dokonca vyradenie servera. Správne navrhnutý mechanizmus ošetrovania a spracovania chýb má vytvárať chybové hlášky (a niektoré z nich logovať) ako dôsledok chyby na webovej stránke, ako aj dôsledok útoku útočníka, ale pritom ich nesprístupniť útočníkovi. Dôležité je ošetrenie všetkých typov chýb a útokov, teda okrem vstupov používateľa aj volanie systému, databázových zadaní či iných interných funkcií. Treba dodržať rovnakú koncepciu spracovania chýb u všetkých spolutvorcov aplikácie. Len veľmi málo webových aplikácií disponuje schopnosťou detekcie intrúzie, v dôsledku čoho nie je väčšina útokov nikdy zachytená. Táto skutočnosť je dôsledkom vážneho podceňovania rôznych útokov. Jednou z možností riešenia je použitie OWASP filtrov (k dispozícii vo viacerých jazykoch), ktoré môžu pomôcť zabrániť prenikaniu chybových kódov do stránok používateľa, ak sú tieto stránky dynamicky vytvárané aplikáciou.

### 8. Nezabezpečené ukladanie údajov – insecure storage

Na ochranu citlivých informácií a prihlasovacích údajov webová aplikácia často používa kryptografické funkcie. Pri integrácii týchto funkcií do aplikácie často dochádza k závažným chybám a podceneniu iných bezpečnostných aspektov, najmä v oblasti nezabezpečenia kryptovania kritických údajov, nezabezpečeného ukladania kľúčov, certifikátov a hesiel, zlej voľby algoritmov a zdrojov náhodných čísel, nezaistení podpory zmeny šifrovacích kľúčov a iných potrebných procedúr údržby a tiež pri pokusoch vyvinúť nové šifrovacie algoritmy. Medzi odporúčané protiopatrenia patrí v prvom rade minimalizácia používania šifrovania na absolútne potrebné informácie a voľba vhodných postupov, napr. namiesto šifrovania a ukladania čísla kreditnej karty stačí použiť opakovaný vstup. Ak sa musí použiť šifrovanie, treba zvoliť verejne preverené knižnice bez známych zraniteľností (dier). Na sťaženie práce útočníka je vhodné rozdeliť hlavný riadiaci kľúč (master secret) aspoň na dve časti a umiestnenia (napr. konfiguračný súbor, externý server, prípadne v samotnom kóde) a zostaviť ho až počas výpočtu.

### 9. Odmietnutie služby – denial of service (DoS)

Spotrebovaním zdrojov webovej aplikácie môže útočník zamedziť prístup používateľov k aplikácii. Medzi tieto (obyčajne limitované) zdroje patrí šírka pásma, pripojenia na databázu, disková pamäť, procesor, pamäť, vlákna alebo iné špecifické zdroje. Iný variant útoku tohto typu je zameraný na konkrétneho používateľa. Útočník môže zablokovať prístup používateľa k jeho účtu alebo môže požadovať nové heslo pre používateľa, a tak ho nútiť k opätovnému prístupu. Niektoré webové aplikácie sú dokonca prístupné útoku, ktorý ich okamžite prepne do offline stavu alebo sa zrútia, čím zabránia všetkým ostatným používateľom ich ďalšie prevádzkovanie. Existuje široké spektrum útokov tohto typu, pričom väčšina z nich môže byť inicializovaná niekoľkými riadkami Perl kódu. Zabrániť útoku typu DoS je ťažké, pretože neexistuje účinná obrana proti nim. Vo všeobecnosti treba limitovať prideľovanie zdrojov na nutné minimum – napríklad stanoviť (pre autentifikovaných používateľov) kvótu pre diskový priestor, spracúvať naraz len jednu požiadavku od jedného používateľa (ďalšiu zahodiť); pre neautentifikovaného používateľa zakázať prístup k databáze a iným zdrojom či rozsiahlejším operáciám.

### 10. Nezabezpečená správa konfigurácie – insecure configuration management

Štandard silnej konfigurácie servera (webového aj aplikačného) je podmienkou bezpečnej webovej aplikácie. Okrem toho aplikačný server poskytuje celý rad služieb (ukladanie dát, adresárové služby, mail atď.), ktoré môže webová aplikácia využívať. Chyby v konfigurácii jedného či druhého servera sa potom môžu prejaviť

v celom rade bezpečnostných problémov webovej aplikácie. Medzi často sa vyskytujúce problémové oblasti patrí napr. nezaplátovaný softvér servera, nezabezpečenie servera (umožňuje listing adresárov), nesprávne prístupové práva k adresárom a súborom, povolenie nepotrebných služieb (správa obsahu, vzdialená administrácia), predvolené účty s predvolenými heslami, povolené administratívne a ladiace funkcie, zlá konfigurácia SSL a šifrovania, použitie predvolených certifikátov, nesprávna autentifikácia s externými systémami. Základným protiopatrením je vytvorenie sprísnených pravidiel konfigurácie webového a aplikačného servera na základe odporúčaní rôznych bezpečnostných organizácií (OWASP, CERT, SANS). Tieto pravidlá obsahujú konfiguráciu všetkých bezpečnostných mechanizmov, vypnutie všetkých nepoužívaných služieb, nastavenie rolí, práv a účtov a zrušenie všetkých defaultov a zmeny príslušných hesiel. Udržiavanie bezpečnej konfigurácie serverov vyžaduje bdelosť a osobnú zodpovednosť, sledovanie aktuálnych bezpečnostných dier a aplikáciu záplat, pravidelné previerky vnútornej i vonkajšej bezpečnosti a tiež pravidelné dokumentovanie celkového bezpečnostného stavu.

## Metodika SANS

SANS (SysAdmin, Audit, Network, Security) Institute v spolupráci s NIPC (National Infrastructure Protection Center) pri FBI asi pred piatimi rokmi vydal materiál Ten Most Critical Internet Security Vulnerabilities, ktorý sa rozšíril medzi tisíckami organizácií. Po tomto materiáli nasleduje Top 20 zatiaľ trikrát a jeho štruktúra sa postupne mení. V r. 2002 obsahoval materiál [11] 7 všeobecných slabín (štandardná inštalácia operačného systému a aplikácií, účty bez hesiel alebo so slabými heslami, neexistujúci alebo nekompletný Backup, veľký počet otvorených portov, nefiltrované pakety prichádzajúcich a odchádzajúcich adries, neexistujúce alebo nekompletné prihlasovanie, zraniteľné CGI programy), 6 slabín pre prostredie Windows (Unicode zraniteľnosť, pretečenie bufera v rozšírení ISAPI, MS IIS Remote Data Service Exploit, NETBIOS – nechránené sieťové zdieľanie, únik informácií cez Null Session Connection – anonymný logon, slabé hešovanie hesiel) a 7 slabín pre prostredie Unix (pretečenie bufera pri vzdialenom volaní procedúr RPC, slabiny programu Sendmail, slabé BIND – Berkeley Internet Name Domain, vzdialené príkazy, LPD – remote print protocol daemon, vzdialená administrácia sadmind a mountd, default SNMP reťazce). Skladba hrozieb a slabín sa priebežne aktualizuje. Aktuálna špecifikácia hrozieb a spôsobov obrany proti nim v poslednej verzii je z r. 2004 [9]. Špecifikácia má tvar zoznamu dvadsiatich bezpečnostných nedostatkov, 10 pre Windows a 10 pre Unix, na ktoré sa viaže najviac úspešných útokov.

### W1. Webové servery a služby – Web Servers&Services

Útok môže spôsobiť odmietnutie služby DoS, vystavenie alebo ohrozenie citlivých dát alebo súborov, vykonanie ľubovoľných príkazov na serveri, prípadne úplné ohrozenie servera. Protiopatrenia – aktuálne updaty a service packs, inštalácia antivírusu a ID (Intrusion Detection), blokovanie nepotrebných skriptov, dôsledné prihlasovanie, odstránenie alebo obmedzenie systémov používaných útočníkmi (ftp, cmd atď.), používanie rôznych konvencií a hesiel na vonkajšom (webovom) a internom systéme. Existujú tiež špeciálne nástroje a postupy pre jednotlivé typy serverov (IIS, Apache, iPlanet), aplikácií (ColdFusion, PerlIIS, PHP) a služieb.

### W2. Služba pracovnej stanice – Workstation Service

Služba Workstation Service zodpovedá za spracovanie prístupu používateľa k lokálnym alebo sieťovým zdrojom (súbor, tlač). Zneužité môže byť pretečenie bufera. Útočník môže získať úplnú kontrolu nad ohrozeným počítačom. Protiopatrenia – aktualizácia záplat, blokovanie portov 139/tcp a 445/tcp, otváranie minimálneho počtu portov, využívanie firewallu, na samostatnom stroji (nie je v sieti) nepovolenie Workstation Service.

### W3. Služby vzdialeného prístupu – Windows Remote Access Services

Rodina operačných systémov Windows podporuje rôzne štandardné sieťové protokoly aj vlastné sieťové metódy a techniky. Na útok sa môžu zneužiť Network Shares, Anonymous Logon, vzdialený prístup k registrom a vzdialené volanie procedúr. Využívanie súborov či adresárov v sieti podporujú protokoly SMB (Server Message Block) a CIFS (Common Internet File System). Účinným protiopatrením je inštalácia Windows XP Service Pack2, ktorý dokáže eliminovať vzdialený anonymný prístup s využitím vzdialeného volania procedúr a celý rad ďalších postupov, členených podľa jednotlivých metód vzdialeného prístupu pre rôzne verzie OS Windows.

### W4. Microsoft SQL Server

MS SQL Server obsahuje niekoľko vážnych slabín, umožňujúcich útočníkovi získať citlivé informácie, zmeniť obsah databázy či ohroziť SQL Server. To využívali rôzne červy a exploity, napríklad už spomínaným pretečením bufera. Protiopatrenia – zakázať SQL/MSDE Monitor Service na UDP porte 1434, dôsledne aplikovať aktuálne opravy a service packy, umožniť zaznamenávanie prihlasovania na server, zabezpečiť server na systémovej aj sieťovej úrovni, minimalizovať privilégiá a riadiť sa príručkou Microsoftu o zabezpečení a bezpečnosti Best Practises.

### W5. Autentifikácia – Windows Authentication

Typické problémy hesiel sú slabé či neexistujúce heslá, chyby používateľov pri ich ochrane, vytváranie účtov operačným systémom alebo aplikáciou so slabým či neexistujúcim heslom, používanie známych hešovacích algoritmov a ukladanie hesiel tak, že je prístupné štandardnému používateľovi. V prostredí Windows existujú tri autentifikačné algoritmy – LM (least secure, most compatible); NTLM a NTLMv2 (most secure and least compatible). LM má viac slabín (dĺžka 14 znakov atď.), a preto môže byť prelomené v relatívne krátkom čase. Protiopatrenia – vytvoriť silné heslo formou kombinácie znakov, číslic a špeciálnych znakov, odolné proti „slovníkovému“ útoku s využitím nástrojov na podporu heslovej politiky, nastaviť vyšší počet zmien hesla (0 – 24), po ktorých sa môže použiť pôvodné heslo, nastaviť maximálny vek hesla (0 – 999 dní), po ktorom heslo exspiruje (0 – nikdy), minimálny vek hesla (0 – 999 dní), po ktorom ho používateľ môže zmeniť (0 – hneď), minimálna dĺžka hesla (0 – 14 znakov), uloženie hesla s využitím reverzibilného šifrovania, udržiavanie politiky silných hesiel v rámci celej organizácie, znemožnenie LM autentifikácie po sieti.

### W6. Webový prehliadač – Web Browser

V prvom rade ide o štandardne nainštalovaný Internet Explorer 6, ktorý má veľký počet bezpečnostných dier – 153 od apríla 2001, dlhý čas, kým sa objaví záplata, možnosť zneužitia ActiveX a Active Scripting prvkov na obídenie bezpečnostných konštrukcií prehliadača, nezabezpečenie voči Spyware a Adware (platí pre všetky prehliadače). Z integrácie IE do OS vyplýva jeho zvýšená napadnuteľnosť. Materiál [9] uvádza (v r. 2004) pre IE 15 bezpečnostných odporúčaní (dier), pre Mozillu 7, pre Netscape 2 a pre Operu 8 vo forme odkazov. Protiopatrenia IE – v prvom rade aktualizácia záplat, najlepšie pomocou automatického režimu, používanie Microsoft Baseline Security Analyser, nepoužívať browser pri prihlásení do systému s právami administrátora, vypnutie funkcie ActiveX. Podobne pri iných typoch prehliadačov treba sledovať ich stránky a používať príslušné záplaty.

### W7. Aplikácie spoločného využívania súborov – File Sharing Applications

Komunikácia P2P (Peer to Peer) zaznamenala veľké až masové rozšírenie. Skladá sa z požiadaviek, odpovedí a prenosu súborov. Súčasne môže prebiehať viac downloadov aj uploadov, čo ľahko vedie k preťaženiu siete. V súvislosti s P2P softvérom existujú tri typy nezabezpečenia – technické (vzdialené zneužitie), sociálne (zmena požadovaného obsahu) a legislatívne (porušenie autorských práv). Protiopatrenia – korporačná stratégia (nesťahovanie autorských materiálov, vhodná stratégia pripojenia na internet, kontrola pamäte a staníc), sieťové obmedzenia (bežný používateľ nemá povolenú inštaláciu softvéru, zvlášť typu P2P, využívanie proxy servera, obmedzenie portov nepotrebných na úradné účely, monitorovanie siete a jej prevádzky, používanie antivírusu a pravidelné aktualizácie).

### W8. Odhalenie – LSAS Exposures

Windows Local Security Authority Subsystem Service v edíciách Windows 2000, Server 2003 a Server 2003 64 Bit, XP and XP 64 Bit obsahuje kritické pretečenie bufera, ktoré v prípade zneužitia môže spôsobiť úplný výpadok systému (platí pre neaktualizovaný Windows a vyžaduje administrátorské práva). Príkladom zneužitia bol napr. W32 Sasser. Protiopatrenia – zablokovanie portov na firewalle, aplikácia aktuálnych záplat od Microsoftu, nastavenie TCP/IP filtrovania s cieľom blokovať prichádzajúcu komunikáciu.

### W9. Poštový klient – Mail Cient

Outlook (O) a Outlook Express (OE) ako základný e-mailový a kontaktný klient je prepojený s Internet Explorerom a ďalšími aplikáciami (Office, BackOffice) aj so samotným operačným systémom. Tým sa vytvára nesúlad so zabudovanými bezpečnostnými mechanizmami a keď k tomu pripočítame ešte aj, jemne povedané, ľahostajnosť koncového používateľa k bezpečnosti, je to dôvod veľkého nárastu červov, e-mailových vírusov, škodlivého kódu a ďalších foriem útokov. Bezpečnostné hrozby zahŕňajú nainfikovanie počítača vírusom alebo červom, nevyžiadanú poštu – spam a overenie správnosti e-mailovej adresy – web beaconing. Protiopatrenia – vhodná konfigurácia minimalizuje bezpečnostné riziká, aplikácia kritických záplat a automatického updatu, nastavenie vysokej bezpečnosti, automatické blokovanie príloh typu exe, com, vbs, výber vhodného typu filtrovania mailov proti spamu (O 2003), čítanie mailov zásadne v textovom formáte (HTML aj RTF môže obsahovať škodlivý kód), nastavenie ochrany proti web beaconing (O 2003), používanie antivírusu a predovšetkým zodpovedné správanie koncového používateľa – neotvárať prílohy, ukladať dokumenty do špeciálneho adresára alebo partície, nastavenie najvyššieho stupňa bezpečnosti a kontrola digitálnych podpisov prílohových súborov.

### W10. Instant Messaging

Rozsiahle možnosti aktuálnych programov IM (vzdialená webová kontrola mailov, hlasový chat, videokomunikácia, posielanie a spoločné využívanie súborov) prinášajú aj zvýšené bezpečnostné riziká veľmi variabilného charakteru (vzdialené pretečenie bufera – RPC, útok založený na URI či zákernej linke, ohrozenie prenosom súborov či ActiveX exploity). Protiopatrenia – aktualizácia IM, nastavenie varovania pri každom prenose súboru, ak je to možné, blokovanie vybraných portov firewallu podľa typu IM programu, blokovanie prístupu k stránkam s nebezpečnými URI (aim:, ymsgr:) a k stránkam vyvolávajúcim ActiveX riadenia.

Špecifikácia Unixových slabých miest.

### U1. Systém doménových mien BIND – BIND Domain Name System

BIND ako najpopulárnejšia implementácia DNS (väzba medzi doménou a IP adresou) je obľúbeným cieľom útokov. Ich variabilita je široká – od DoS cez pretečenie bufera až po znehodnotenie cache pamäte – cache poisoning. Protiopatrenia – aktualizácie, záplaty, aplikácia vhodných firewallových pravidiel, zabezpečenie šifrovaných prenosov medzi primárnym a sekundárnym serverom, používanie TSIG (DNS Transaction Signatures) a dodržiavanie ďalších bezpečnostných pravidiel podľa návodov.

### U2. Web Server

Ich slabiny sa týkajú servera samotného, ako aj rôznych prídavných modulov a skriptov. Výsledkom útoku môže byť DoS, poškodenie stránok či dokonca úplný rootovský prístup útočníka na server. Protiopatrenia – aktualizácie, záplaty, znemožnenie všetkých nepotrebných funkcií servera, zabezpečenie potrebných funkcií (secure mode, mod_security proti XSS a SQL injection), prevádzka servera bez super-user privilégií, obmedzenie serverom poskytovaných informácií – zablokovať mod_info pre prístup z internetu.

### U3. Autentifikácia – Authentication

Slabé, žiadne alebo všeobecne známe heslá na strane používateľov, administrátorských účtov a šifrovacích algoritmov. Protiopatrenia – silná politika hesiel s detailnými inštrukciami s kompletnou podporou organizácie, prísna kontrola účtov a hesiel, používanie šifrovacích programov a protokolov, znemožnenie vzdialeného logovania administrátora a minimalizovanie používania tohto účtu a hesla, dôsledné zaznamenávanie a vyhodnocovanie všetkých (úspešných i neúspešných) pokusov o prihlásenie.

### U4. Systém kontroly verzií – Version Control Systems

Najčastejšie sa využíva systém CVS (Concurrent Versions System) s protokolom pserver, výrazné rozšírenie má tiež systém Subversion s protokolom svn. V oboch prípadoch môže dôjsť k útoku pretečením pamäte (heap-based overflow), autentifikovaným aj anonymným útočníkom (DoS na CVS serveri, vykonanie ľubovoľného kódu na serveri). Protiopatrenia – štandardná aktualizácia, záplaty, pre CVS namiesto pserver využiť SSH protokol, pre Subversion namiesto svn webDAV prístup, prevádzkovať server pre anonymný read-only prístup na nezávislom systéme.

### U5. Mail Transport Service

MTAs (Mail Transport Agents) zodpovedajú za prenos e-mailov a vďaka rozsiahlemu využívaniu mailov sú vystavené stálym útokom (voči systému bez záplat – pretečenie bufera, pamäte, zneužitie prenosovej cesty – spamy a iných neprenosových faktorov – databáza účtov používateľov). Nezabezpečené MTAs je takmer okamžite napadnuté. Protiopatrenia – prevádzka Mail Servera len na vyhradenom a autorizovanom serveri, aplikácia vhodnej firewallovej politiky, záplaty, upgrady, oddelený MTA na vnútornú poštu, limitovanie privilégií MTA, dodržiavanie pokynov a dokumentácie, špecifické opatrenia podľa typu MTA – pre Sendmail, Qmail, Courier-MTA, Exim, Postfix atď.

### U6. SNMP – Simple Network Management Protocol

Všadeprítomný SNMP je vo verziách 1, 2 a 3, pričom mnoho predajcov ešte stále ako preddefinovanú voľbu dáva v1. Bezpečnostný model verzie 3 využíva vylepšenú metódu autentifikácie. Slabiny najmä v1 a v2 môžu byť zneužité na vzdialenú rekonfiguráciu či ukončenie činnosti zariadenia. Sledovanie SNMP môže odhaliť veľa informácií o štruktúre siete a pripojených systémov a zariadení. Protiopatrenia – kdekoľvek je to možné používať v3 s autentifikáciou správ a šifrovaním dátových jednotiek protokolu, filtrovať prístupové body do siete, blokovať neželané SNMP požiadavky, komunikácia len medzi dôveryhodnými podsieťami.

### U7. Open Secure Socket Layer SSL

Knižnica OpenSSL je integrovaná s celým radom aplikácií a protokolov (Apache, POP3, IMAP, SMTP, LDAP), preto môžu byť

cez jej slabiny napadnuté. Protiopatrenia – upgrade na najnovšiu verziu OpenSSL, záplaty, použitie ipfilter/netfilter alebo iných firewallových nástrojov.

### U8. Zlá konfigurácia služieb – Misconfiguration of Enterprise Services NIS/NFS

Network File System (NFS) a Network Information Service (NIS) zabezpečujú spoločné využívanie súborov a adresárov v sieti, a preto sú štandardným cieľom útokov (DoS, pretečenie bufera, slabá autentifikácia). Protiopatrenia – využiť všetky bezpečnostné parametre a možnosti, explicitne označiť NIS servera v pripájajúcich sa klientoch, komunikácia NIS s klientmi len cez privilegované porty, NFS používať IP adresy alebo plné doménové názvy namiesto aliasov, obmedziť prístup k súborovému systému NFS, využiť nástroj NFSBug na overenie konfigurácie NFS, používať bezpečný protokol, firewall, záplaty a aktuálne verzie.

### U9. Databázy – Databases

Všetky moderné relačné databázové systémy sú adresovateľné cez port (Oracle TCP 1521, MySQL TCP 3306, PostgreSQL TCP 5432), čo umožňuje pokusy o priame pripojenie k databáze s obchádzaním bezpečnostných mechanizmov operačného systému. Mnohé databázové systémy majú známe predvolené účty a heslá a samozrejmosťou je webový prístup. Nedostatky konfigurácie databázy a zle zostavenej (nezabezpečenej) aplikácie vytvárajú možnosti rôznych útokov (vloženie SQL, exploity, atď.). Protiopatrenia – aktualizácia verzií, bezpečná prevádzka – systém privilégií, odstrániť predvolené heslá na db a systémových účtoch, kontrolovať dĺžku všetkých formulárových vstupov a validovať ich na strane servera (dĺžku, formát, typ), využívať uložené (stored) procedúry a vylúčiť nevyužívané, využívať bezpečnostné opatrenia výrobcov a bezpečnostných organizácií (OWASP, CERT, SANS).

### U10. Jadro – Kernel

Pretože jadro je centrom operačného systému (má privilegovaný prístup k všetkým jeho zložkám), jeho zneužitie je zvlášť nebezpečné (DoS, vykonanie ľubovoľného kódu, neobmedzený prístup k súborovému systému, vzdialené zneužitie). Protiopatrenia – naladenie systémových zdrojov tak, aby obmedzovali DoS útoky a pretečenia bufera, sprísnenie nastavení sieťovej konfigurácie voči sieťovým útokom. Pretože príkazy a parametre konfigurácie sú platformovo závislé, treba sa riadiť príslušnou dokumentáciou. Množstvo odkazov je v [9].

## Metodika US-CERT

US-CERT (United States Computer Emergency Readiness Team) je pracovisko Carnegie Mellon University CERT/CC (Computer Emergency Response Team/Coordination Center) založené v r. 1988, zamerané na zlepšovanie internetovej bezpečnosti. Je podporované U.S. Department of Defense. Každoročne publikuje množstvo bezpečnostných odporúčaní (vulnerability notes), ktoré vytvárajú databázu poznatkov a odporúčaní [3]. V tejto databáze možno vyhľadávať podľa viacerých kľúčov (napr. názov, identifikátor napadnuteľnosti, názov CVE – Common Vulnerabilities and Exposures, dátum aktualizácie, dátum publikovania a i.) [12]. CERT/CC sa zameriava na poskytovanie technického poradenstva, koordináciu reakcií na bezpečnostné incidenty a veľké udalosti, spoluprácu s inými bezpečnostnými expertmi a organizáciami, identifikáciu trendov aktivít útočníkov, diseminácia informácií pre širokú komunitu, analýzu napadnuteľnosti produktov a škodlivého kódu, publikáciu technickej dokumentácie, poskytovanie tréningových kurzov a podporu vedúceho postavenia v komunite riešenia útokov. Podrobnejší prehľad aktivít CERT-u, súčasného stavu internetovej bezpečnosti, typov škodlivých útokov, aktuálnych slabín a metód útokov, bezpečnostných politík stránok a ošetrenia incidentov stránok uvádza vo forme modulov stránka [2]. Vývoj počtu bezpečnostných odporúčaní od r. 1998 ilustruje tab. 1.

| rok | 1998 | 1999 | 2000 | 2001 | 2002 | 2003 | 2004 |
|---|---|---|---|---|---|---|---|
| Vulnerability Notes | 8 | 3 | 47 | 326 | 375 | 255 | 341 |

**Tab.1**

## Iné metodiky

Do úsilia o zvýšenie bezpečnosti operačných systémov, aplikácií, webových aplikácií aj používateľov sa zapájajú aj ich najvýznamnejší výrobcovia a dodávatelia. Na jednom z popredných miest je firma Microsoft so svojou iniciatívou Trustworthy Computing [7]. Tá je založená na štyroch základných pilieroch – bezpečnosť (Security), súkromie (Privacy), spoľahlivosť (Reliability) a úcta k zákazníkovi (Business Integrity). Špecifikácia dôvodov útokov a kvalifikácie útočníkov je znázornená na obr. 1, ktorý dáva odpoveď na otázku, kto útočí a prečo útočí na bezpečnosť webových aplikácií a informačných technológií. Od r. 1991 je na svete (a, žiaľ, aj sa dosť používa) pojem digitálny Pearl Harbor s významom zdrvujúci bezpečnostný incident, spojený s obrovským výpadkom počítačov a veľkou finančnou stratou. Stal sa synonymom vety: „Teroristi vypnú internet."

| KTO / PREČO | začiatočník | pokročilý | expert | špecialista |
|---|---|---|---|---|
| kuriozita | VANDAL | | AUTOR | |
| osobná sláva | | NARUŠITEĽ | | |
| osobný prospech | | ZLODEJ | | |
| národný záujem | | | ŠPIÓN | |

**Obr.1 Kategórie útočníkov**

Z celosvetového prieskumu stavu informačnej bezpečnosti [1] vyplynulo, že kontrola informačnej bezpečnosti oddelením IT je limitujúcim faktorom jej zlepšovania, a preto je vhodné odobrať ju z kompetencií IT. Nevyhnutnosť stanovenia, investovania a vykonávania vhodnej bezpečnostnej politiky je daná faktormi ochrany stability firmy, úsporami financií, dodržiavaním zákonných predpisov a smerníc, definovaním pravidiel a zodpovednosti v riadnej aj mimoriadnej situácii, minimalizáciou škôd, ochranou citlivých informácií a obmedzovaním absolútneho rozhodovania (administrátor, manažér).

## Záver

Bezpečnosť webu a webových aplikácií je komplexná téma, ktorá zahŕňa bezpečnosť počítačových systémov, sieťovú bezpečnosť, autentifikačné služby, overovanie správ, otázky ochrany súkromia, ako aj problematiku šifrovania. Vo všetkých týchto oblastiach sa pomerne často ukazujú rôzne slabiny, diery či nezabezpečenia, ktoré sa okamžite stávajú predmetom útokov a záujmu útočníkov. Výrobcovia a dodávatelia jednotlivých riešení rôznymi metódami (aktualizácie, záplaty) zistené nedostatky eliminujú, je však veľmi dôležité zabezpečovať čo najrýchlejší prenos týchto riešení na príslušné počítačové vybavenie organizácie. Všetko je v ľuďoch, preto treba viesť administrátorov aj všetkých používateľov IKT k ich správnemu, zodpovednému a bezpečnému využívaniu.

## Literatúra

[1] BERINATO, S., COSGROVE, L., FREJTICHOVÁ, J.: 2004 Digitální bezpečnost. Business World č. 3, 2004, IDG Czech, a. s., Praha, ISSN 1213-1709, s. 6 – 11.

[2] CERT/CC Overview Incident and Vulnerability Trends [internet] 15.5.2003 [30.3.2005] <http://www.cert.org/ present/cert-overview-trends/>

[3] CERT/CC Statistics 1988-2004 [internet] 24.1.2005 [30.3.2005] <http://www.cert.org/ stats/cert_stats.html>

[4] DEVÁT, J.: 2002 Objevme svůj potenciál v digitálním světě! [internet] október 2002 [30. 3. 2005] <http://digiweb.cz/index.php?p=i00000_save&a%5Bid%5D=11647340&a%5Barea_id%5D=10074080>

[5] DOUCEK, P.: 2005 Bezpečnost IS/ICT a proces globální integrace. AT&P journal priemyselná automatizácia a informatika č. 1, 2005, ročník 12, HMH, s. r. o., Bratislava, ISSN 1335-2237, s. 65 – 68.

[6] HRDINA, L.: Deset hlavních slabin webových aplikací a jejich zabezpečení. IT Systems, CCB, s. r. o, Brno, ročník 7, č. 1 – 2, 2005, ISSN 1212-4567, s. 58 – 61.

[7] LIPNER S., HOWARD, M.: 2005 The Trustworthy Computing Security Development Lifecycle [internet] March 2005 [30.3.2005] <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnsecure/html/sdl.asp>

[8] OWASP The Ten Most Critical Web Application Security Vulnerabilities 2004 Update. [internet] 27.1.2004 [3.3.2005] <www.owasp.org/documentation/topten>

[9] SANS Top 20 Internet Security Vulnerabilities 2004 Updated [internet] 8.10.2004 [3.3.2005] <http://www.sans.org/top20/>

[10] TELEPOVSKÁ, H.: 2004 Štandardy ochrany a bezpečnosti informácií. AT&P journal priemyselná automatizácia a informatika č. 12, 2004, ročník 11, HMH, s. r. o., Bratislava, ISSN 1335-2237, s. 49 – 52.

[11] The Twenty Most Critical Internet Security Vulnerabilities 2002 [internet] 2. 5. 2002 [30. 3. 2005] <http://www.sans.org/top20/top20_oct01.php>

[12] US-CERT Vulnerability Notes 2005 [internet] [30. 3. 2005] <http://www.kb.cert.org/vuls>

[13] W3C Security Resources. [internet] 1999 [30. 3. 2005] <http://www.w3.org/Security/>

*Príspevok je riešený v rámci projektu KEGA 3/3084/05, KEGA 1/3126/05 (B), KEGA 1/3124/05 (L) a VEGA 1/2179 /05 (D).*

**Pavel Horovčák**

**Technická univerzita**
**Fakulta Baníctva, ekológie, riadenia a geotechnológií**
**Katedra informatizácie a riadenia procesov**
**Boženy Němcovej 3**
**040 00 Košice**
**Tel: 055/602 51 76**
**e-mail: Pavel.Horovcak@tuke.sk**