E-DROŠĪBAS PROBLĒMAS UN AIZSARDZĪBAS METODES
E-SAFETY PROBLEMS AND PROTECTION METHODS

Autore: **Kristiāna INĶĒNA**, e-pasts: kristiana.inkena@inbox.lv, tālrunis: 26588672
Zinātniskā darba vadītājs: **Sergejs Kodors, Dr.sc.ing.**, sergejs.kodors@rta.lv
Rēzeknes Tehnoloģiju akadēmija
Atbrīvošanas aleja 115, Rēzekne, LV-4601

Abstract. *E-security is the protection of all data stored on computer networks and computer systems against damage, loss or unauthorized access. E-security, based on the definition, is all that can be related to the safe use of the Internet, personal knowledge and behavior, and ethics on the Internet.*

There are examined following threats to websites - the leakage of information, cross-site scripting attacks, injection, unsafe direct object reference, CSRF, security configuration errors, unsafe cryptographic repository, and redirection and transmission without validation.

The author reviews the cyber attacks recorded in Latvia during this year, as well as statistics on recorded incidents during the last year.

The final chapter of the work provides a table that summarizes methods and tools for protecting websites from attacks.

Keywords: *cyber security, e-safety problems, e-safety protection methods.*

Ievads

Drošība e-vidē ir visa datortīklos un datorsistēmās uzglabāto datu aizsardzība no bojājumiem, zaudēšanas vai nesankcionētas piekļuves. E-drošība, balstoties uz definīciju, ir viss, ko var saistīt ar droši interneta izmantošanu, personas zināšanām un rīcībām, kā arī ētiku interneta vidē. Tehnoloģiskā datu aizsardzība, kā, piemēram, programmatūras, vīrusu aizsardzība, ir definējamas kā e-aizsardzība.

Jebkurš uzbrukums datiem, sākotnēji tiek izplānots. Uzbrukumu princips parasti ir sekojošs – tiek izpētīta esošā situācija, tiek veikta skanēšana, tiek iegūta piekļuve, piekļuve tiek izmantota un beigās tiek slēptas pēdas par uzbrukumu. [1]

Darba mērķis ir izvērtēt pastāvošos draudus tīmekļa vietnēm un apskatīt drošības risinājumus, kā arī izpētīt statistiskos datus par drošības incidentiem Latvijā.

Internets ir kā platforma, kurā notiek milzīga informācijas aprite, un ja informācija nav speciāli šifrēta, tā var nonākt tādu personu rokās, kas to var izmantot ļaunprātīgi. Īpaši augsts risks ir gadījumā, kad personas izmanto bezvadu tīklu – atrodoties signāla zonā, šos datus var pārtvert teju ikviens ļaundaris.

Mūsdienās aktuālākie interneta vidē pastāvošie draudi tīmekļa vietnēm ir šādi:

- Informācijas noplūde
- Starpvietņu skriptošanas (*XSS*) uzbrukumi
- Injekcijas
- Nedroša tiešā objektu norāde
- *CSRF*
- Drošības konfigurācijas kļūdas
- Nedroša kriptogrāfiskā glabātuve
- Novirzīšana un pārsūtīšanas bez validācijas. [2]

Materiāli un metodes

Darbā izmantota monogrāfiska jeb aprakstoša metode, darbam izmantoti statistiskie dati no Informācijas tehnoloģiju drošības incidentu novēršanas institūcijas „CERT.LV”.

Draudi tīmekļa vietnēm

Informācijas noplūde un nekorekta sesiju pārvaldība apdraud visus uzņēmumus, kuriem ir tīmekļa vietne, kurā reģistrējas klienti. Izmantojot trūkums autentifikācijas procesā, uzbrucējs

http://dx.doi.org/10.17770/het2018.22.3639

var izlikties par citu lietotāju un tādā veidā var iespaidot citu personu kontus. Tiklīdz uzbrucējs ir ieguvis pieeju svešam kontam, viņš var veikt nelikumīgas darbības lietotāja vārdā. Visbiežāk uzbrucējs mēģina piekļūt, piemēram, sistēmas administratora piekļuvei, jo tādā veidā kaitnieciskais mērķis var tikt vieglāk sasniegts. Uzbrucēji nereti ir ne tikai anonīmi lietotāji no malas, bet arī reģistrēti lietotāji vai pat uzņēmuma darbinieki. [2]

Šāda veida draudi visbiežāk tiek īstenoti, ja uzņēmuma tīmekļa vietnei ir nepilnīga lietotāju autentifikācijas sistēma, vai arī tiek sesiju pārvaldīšanas nenotiek augstā līmenī, kas rada nepilnības, piemēram, paroles pārvaldībā, atslēgšanās no sistēmas, automātiska atslēgšanās no sistēmas pēc konkrēta neaktīva laika perioda, konta atjaunināšana, paroles atcerēšanās u.c. tamlīdzīgās jomās. [2]

Ja sesijas identifikators tiek saglabāts kā daļa no saites, tad līdz ar „http://www.abcd.com" pie saites parādās arī, piemēram, „AfePEYj6oBs8CWZgnlvrKu-S-m-vFdbtmcXu_LPSbHrp" un persona, pavisam nejauši nosūta citai personai papildus informāciju – sesijas identifikatoru, pēc kura sistēmas var atpazīt lietotāju. Šādā veidā persona var nosūtīt sava profila informāciju citai personai.

Ja persona izmanto publiski pieejami datoru, un tīmekļa vietnei ir uzstādīta pārāk ilga automātiskā atslēgšanās no sistēmas, ir iespējama situācija, kad persona nepiespiež „*Log Out"*, tā vietā tikai aizverot pārlūkprogrammu un rezultātā nākamā persona, kura nonāk pie šī datora, bez ielogošanās un paroles sniegšanas, tiek automātiski atpazīta kā iepriekšējā persona.

***XSS* uzbrukumus** var veikt, ja tīmekļa lapai ir kāda datu ievades forma, kaut vai tikai komentāru sadaļa. Ja tīmekļa vietne nav aizsargāta pret šāda veida uzbrukumiem, uzbrucējs, ievadot tekstu, ko sastāda kods, principā saglabā tīmekļa vietnē savu programmu, kura izpildās lietotāju pārlūkprogrammās un tādā veidā uzbrucējs iegūst lietotāju datus – lietotājvārdu, paroli vai jebkādus citus datus. Šāda veida uzbrukumi sastāda lielu daļu drošības incidentu tīmekļa vietnēs un lai gan parasti mērķis ir lietotājs, ir atsevišķi gadījumi, kad cieš arī pati vietne. Šāds risks pastāv, ja tīmekļa vietnē ir ievades forma, kas ierakstus publicē bez filtrēšanas. [2]

Piemēram, ja komentāru sadaļā kāds konkurents ierakstīts komentāru ar kodu, kas nosaka paziņojuma parādīšanos, katru reizi apmeklējot lapas komentāru sadaļu, pārlūkā parādīsies uzbrucēja izvēlēts ziņojums, kas kaitēs tīmekļa vietnei un reklamēs konkurentu.

Tāpat arī ja tīmekļa vietne izmanto sīkdatnes un nav aizsargāta pret *XSS* uzbrukumiem, uzbrucējs var piekļūt personas datiem un tos ļaunprātīgi izmantot.

***SQL* injekcijas** ir populārs uzbrukuma veids, ja uzbrucējs plāno uzbrukt tīmekļa vietnes datu bāzei. Tāpat kā *XSS* uzbrukumos, parasti tiek uzbrukts caur datu ievades formu tīmekļa vietnē, taču ne tikai – *SQL* injekcijas var notikt arī caur *URL*. Ievadītos uzbrucēja datus apstrādā datu bāze un tādā veidā uzbrucējs iegūts piekļuvi datu bāzē esošajai informācijai, to labot, dzēst, izpildīt darbības administratora vārdā. Visbiežāk šādi uzbrukumi izdodas gadījumos, ka tīmekļa vietnes ievades datus nevalidē. [2]

Nedroša tiešā objekta norāde nozīmē, ka **t**īmekļa lapu ģenerēšanas procesā, tiek izmantots faktiskais objekta vārds jeb atslēga. Autorizēti sistēmas lietotāji, izmainot kāda parametra vērtību, no viena sistēmas objekta, kas norāda uz nākamo sistēmas objektu, var nonākt pie tādas informācijas, kura nav lietotājam pieejama. Uzbrukums izpildās, ja tīmekļa vietne lieto neverificētus datus *SQL* vaicājumā. Šāda parametra izmainīšana var iespaidot visu datus, uz kuriem attiecināms izmainītais parametrs. Ja parametra vērtība ir vienkārša, kā, piemēram, burti vai skaitļi, uzbrucējs salīdzinoši viegli piekļūst veselām datu kopām. [2]

CSRF uzbrukums ir izplatīts gadījumos, kad uzbrucējs var paredzēt visas lietotāja darbības. Uzbrucējs sagatavo viltojumu – *HTTP* pieprasījumu un panāk, ka lietotājs to nosūta, izmantojot dažādus līdzekļus. Ja lietotājs šo darbību veic autorizējies tīmekļa vietnē, uzbrukums panāk rezultātu. Uzbrukuma rezultātā, lietotājs, pats nezinot, var veikt izmaiņas savos vai sev pieejamajos datos. [2]

Piemēram, uzbrucējs var izveidot pieprasījumu naudas pārvedumam no lietotāja konta uz upura kontu un šo pieprasījumu izvietot tīmekļa vietnē, ko regulē uzbrucējs. Gadījumā, kad

lietotājs šo vietni apmeklē, vienlaicīgi būdams autorizējies savā internetbankā, pieprasījums tiek izpildīts.

Drošības konfigurācijas kļūdas gadījumos, tīmekļa vietnes ievainojamība var izpausties gan tīmekļa serverī, gan platformā, gan programmas kodā. Uzbrukuma laikā uzbrucējs var izmantot noklusējuma kontus, neizmantotas lapas, neaizsargātus failus u.c. vietas, lai nodrošinātu sev neautorizētu piekļuvi sistēmas daļām vai datiem. [2]

Nedroša kriptogrāfiskā glabātuve var kļūt par uzbrukuma upuri, ja uzbrucējs ir sistēmas lietotājs. Ārējie uzbrucēji izvēlas citus uzbrukuma kanālus, jo ir sarežģīti atklāt vājos punktus bez pieejas. Bieži sastopama situācija, kad dati, kuriem būtu jābūt šifrētiem, netiek šifrēti, vai arī tiek šifrēti ar nedrošām atslēgām vai glabāti neatbilstošās vietās. [2]

Piemēram, uzņēmums izveido datu bāzes rezerves kopiju, šifra atslēgu saglabājot kopā ar datu bāzes kopiju. Uzbrucējs pavisam vienkārši tiek pie datu bāzes datiem.

Novirzīšana un pārsūtīšana bez validācijas nozīmē to, ka uzbrucējs izveido saiti uz drošu vietni, lietotājs noklikšķina, un nedrošas pārsūtīšanas rezultāta, uzbrucējs ir ticis garām drošības pārbaudēm. Nedrošas novirzīšanas rezultātā, uzbrucējs var atstāt lietotāja datorā programmatūras, kas darbojas ļaunprātīgos nolūkos. [2]

Ņemot vērā, ka sabiedrība kopumā paliek arvien informētāka par datu drošību interneta vidē, arī ļaunprātīgo programmu veidotāji ir spiesti mainīties un pielāgoties. Tā, piemēram, diezgan sastopama šobrīd ir *scareware* jeb latviskojot „baidatūra". Tā ir programmatūra, kas paziņo datora lietotājam, ka dators ir nedrošs un rosina lejupielādēt programmu, kas it kā palīdzēs tikt galā ar vīrusiem. Tādā veidā uzbrucējs pierunā lietotāju lejupielādēt ļaunprātīgu programmatūra, kas pēc tam datorā veic sev vēlamās darbības. [3]

Incidentu statistika

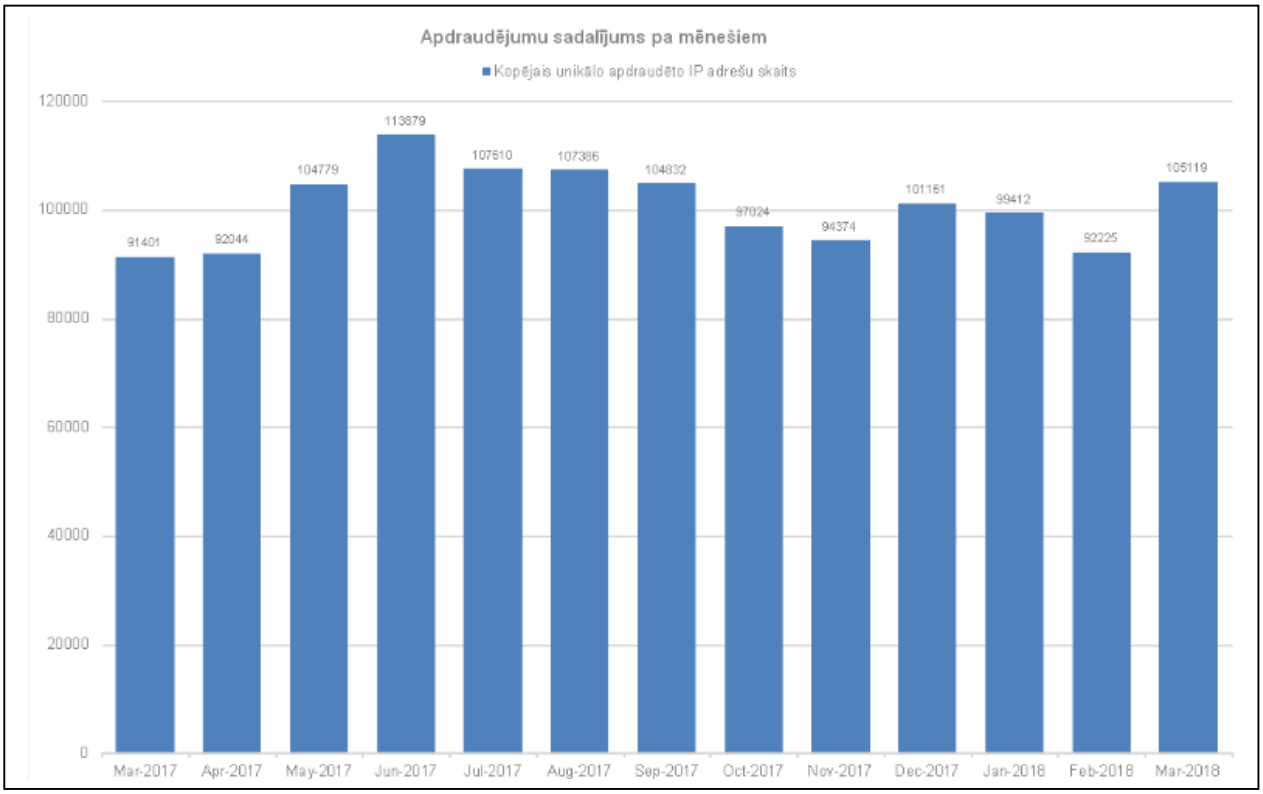
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija „CERT.LV" šī gada martā ir konstatējusi sekojošus incidentus:

- 78 279 IP adresēs konfigurācijas nepilnības
- 17 854 IP adresēs ļaundabīgs kods
- 87 IP adresēs ielaušanās mēģinājumi
- 41 IP adresē krāpšana
- 32 IP adresēs kaitīgs saturs
- 24 IP adresēs kompromitētas iekārtas
- 10 IP adresēs informācijas vākšana. [4]

1.attēlā redzams, ka incidentu skaits Latvijā pēdējā gada laikā ir bijis salīdzinoši vienmērīgs. Vidēji katru mēnesi ir reģistrētas 100810 IP adreses, kurās noticis incidents.

17. janvārī uzbrukumu piedzīvoja informācijas aģentūra LETA. Lai gan uz vairākām stundām piekļuve mājaslapai bija apgrūtināta, uzbrukums tika novērsts. Uzbrukums analogs e-veselības uzbrukumam – mērķtiecīgi plānots, milzīgs pieprasījumu skaits no dažādām valstīm. [6]

3. martā par mērķtiecīgu ārējo uzbrukumu mājaslapai paziņoja „Biļešu paradīze". Zīmīgi, ka tieši šajā dienā uzņēmums sāka biļešu pārdošanu uz Dziesmu un deju svētku pasākumiem. Biļetes iegādes process internetā aizņēma vairākas stundas un, sakarā ar uzbrukumu, pat pēc vairāku stundu gaidīšanas, daļa pircēju pie biļetēm netika. Uzņēmuma vadītājs Ēriks Naļivaiko intervijā atturējās no komentāriem par to, kāds ir uzbrukuma mērķis, uzsverot, ka paziņojis informācijas tehnoloģiju drošības incidentu novēršanas institūcijai „CERT.LV". [7]



1.attēls. **CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 12 mēnešu griezumā**

Metodes tīmekļa vietņu aizsardzībai

1.tabula

Draudi tīmekļa vietnēm un metodes, kā aizsargāties no uzbrukumiem [2]

Drauds	Metodes, kā aizsargāt
Informācijas noplūde	Jāaizsargā autentifikācijas dati un sesiju identifikatori. Jāšifrē lietotāju autentifikācijas dati. Jānodrošina, ka sesijas identifikatori nav attēloti saitē. Jānodrošina automātiska atslēgšanās no sistēmas pēc konkrēta pasīva laika perioda. Jāģenerē sesijas identifikators uzreiz pēc autentifikācijas.
Starpvietņu skriptošanas (*XSS*) uzbrukumi	Jāatdala neuzticami dati no aktīvā pārlūka satura. Jānodrošina datu pārbaude un filtrēšana, pirms dati tiek attēloti tīmekļa vietnē, kā arī jānodrošina, ka ievaddatus uztver kā tekstu, nevis izpildāmu saturu. Jāizmanto ievaddatu filtrēšana, balstoties uz attiecīgo programmēšanas valodu. Jāatkodē kodētie ievaddati un jāformatē atbilstoši noteiktajam.
Injekcijas	Jāatdala neuzticami dati no komandām un vaicājumiem. Ar testēšanas rīku palīdzību, kontrolētā veidā var veikt uzbrukumus, lai pārbaudītu tīmekļa vietnes drošību. Jāizmanto drošs *API*, kas nodrošina funkcionalitāti izmantot parametrizētu interfeisu. Jāizmanto ievaddatu validēšana, izvairoties no īpašiem simboliem.

Nedroša tiešā objektu norāde	Jāpārbauda objektu norāžu aizsardzība. Jāpārbauda resursa pieejamība konkrētam lietotājam. Reti kurš automatizēts drošības pārbaudes rīks spēs noteikt objektu norādes drošību, jāveic manuāla testēšana.
CSRF	Jāpārbauda vai saites, kas veic stāvokļa maiņas funkcijas, ir drošas. Jāpaplašina vairāku soļu transakcija.
Drošības konfigurācijas kļūdas	Nodrošināt identiskas izstrādes, kvalitātes nodrošināšanas un produkcijas vides. Izstrādāt tādu sistēmas arhitektūru, kas nodala komponentes no drošības. Jāveic regulāras auditācijas.
Nedroša kriptogrāfiskā glabātuve	Noteikt, kuri dati ir pietiekami svarīgi, lai būtu šifrējami. Izmantot šifrēšanas algoritmus. Jāizveido droša atslēga, kā arī jāparedz periodiskas atslēgas maiņas. Jāšifrē visas datu rezerves kopijas.
Novirzīšana un pārsūtīšanas bez validācijas	Nenorādīt parametru, kas nosaka galamērķi, datu novirzīšanas un pārsūtīšanas gadījumos. Ja parametru ir nepieciešams norādīt, tad šo parametru neizmanto kā faktisku saiti.

Rezultāti un to izvērtējums

Darba autore ir sasniegusi izvirzīto mērķi, darbā ir definēti aktuālākie interneta vidē pastāvošie draudi tīmekļa vietnēm un darba noslēguma nodaļā ir uzskaitīti izstrādātie ieteikumi, lai izvairītos no uzbrukumiem un incidentiem. Vissarežģītākais uzdevums darba procesā bija definēt pastāvošos draudus, jo nozares straujā attīstība un dinamika ir tik mainīga, ka pat identificēti draudi, kombinācijā ar citiem līdzekļiem, var radīt jaunus draudus.

Secinājumi

Ņemot vērā, ka sabiedrība kopumā paliek arvien informētāka par datu drošību interneta vidē, arī ļaunprātīgo programmu veidotāji ir spiesti mainīties un pielāgoties un šis process pastāvēs vienmēr. Darba autore secina, ka pastāv daudz risku tīmekļa vietnēm, taču veicot dažādas pārbaudes un nodrošinoties pret tiem, lielākā daļa risku ir novēršami. Sadarbojoties uzmanīgam interneta lietotājam un apzinīgam tīmekļa vietnes uzturētājam, veidojas drošs tandēms.

Summary

In this paper there are examined following threats to websites - the leakage of information, cross-site scripting attacks, injection, unsafe direct object reference, CSRF, security configuration errors, unsafe cryptographic repository, and redirection and transmission without validation.

The goal of the work is to assess the existing threats to websites and develop solutions, as well as to study the statistical data on security incidents in Latvia.

Any attack on data is initially planned. The attack principle is usually the following: the current situation is being investigated, scanning is done, access is obtained, access is used and the traces of attack are finally hidden.

The number of incidents in Latvia during the last year has been relatively even. On average, 100810 IP addresses are registered each month in which an incident occurred.

The last three major attacks on security systems in Latvia are an attack on the e-health systems, an attack on the homepage of the agency LETA and the "Ticket Paradise" homepage.

On January 16, the e-health system stopped working because of an attack aimed at paralysis of the system, indicating that it was not able to protect itself. The Distributed Service Blocking Method (DDoS) was used to attack - it generates several tens of thousands of requests per second, mostly from Andalucía, Trinidad and Tobago. After the results of the investigation it was confirmed that nobody entered the system and no personal data was obtained.

On January 17, an information agency LETA experienced an attack. Although access to the homepage was difficult for several hours, the attack was prevented. Attack was an analogue to e-health attack - targeted, huge number of requests from different countries.

On March 3, the "Ticket Paradise" was announced for a targeted external attack on the website. It is noteworthy that on this very day the company began selling tickets for the Song and Dance Festival events. The ticket purchase process on the Internet lasted several hours and, due to the attack, even after several hours of waiting, some purchasers did not get the tickets.

The general public is increasingly aware of the security of data in the Internet environment, malware makers are also forced to change and adapt, and this process will always exist. The author concludes that there are many risks to websites, but most of the risks can be eliminated by performing various checks and assisting them. Working with a careful internet user and a dedicated website maintainer, a tandem is certain.

Literatūra

1. Jeremy, Mr Swinfen Green, *Cyber Security*, Gower: Ashgate Publishing, Ltd 2015. 246 lpp.
2. Gori U., *Modelling Cyber Security: Approaches, Methodology, Strategies*, Amsterdam: Amsterdam IOS Press 2009. 2015 lpp.
3. Peter R.J. Trim, *Cyber Security Culture, Counteracting Cyber Threats Through Organizational Learning and Training*, Routledge 2016. 234 lpp.
4. https://cert.lv/lv/incidenti/statistika Sk.internetā (18.04.2018)
5. https://www.lsm.lv/raksts/zinas/latvija/cert-uzbrukums-e-veselibai-visticamak-ir-pasutits.a264709/ Sk.internetā (18.04.2018)
6. https://www.lsm.lv/raksts/zinas/latvija/noticis-kiberuzbrukums-zinu-agenturai-leta.a264633/ Sk.internetā (19.04.2018)
7. https://www.lsm.lv/raksts/zinas/latvija/bilesu-paradize-majaslapas-darbibas-atrumu-ietekmejis-arejs-uzbrukums.a270087/ Sk.internetā (19.04.2018)