Neklasificēšanas pamatojums:
VARAM 07.11.2024. vēstule
Nr.1-13/6547

~~„DIENESTA VAJADZĪBĀM"~~

NAV KLASIFICĒTS

Projekts

I.Stafecka
11.04.2024.

Informatīvais ziņojums
„Par tīmekļa vietņu drošības paaugstināšanu"

Informatīvais ziņojums „**Par tīmekļa vietņu drošības paaugstināšanu**" izstrādāts pamatojoties uz Ministru kabineta 2010.gada 5.maijā sēdes protokollēmumu (prot. Nr.22 26.§, TA - 939). Informatīvais ziņojums „**Par tīmekļa vietņu drošības paaugstināšanu**" satur informāciju par drošības pārbaudē atklātiem apdraudējumiem un rekomendācijas to novēršanai, kā arī ieteikumus vietņu drošības paaugstināšanai.

2009.gadā Īpašu uzdevumu ministra elektroniskās pārvaldes lietās sekretariāts (turpmāk – Sekretariāts) pamatojoties uz Ministru kabineta 2008.gada 19.februāra sēdē (prot. Nr.11 4.§) 7.6.3.apakšpunktā doto uzdevumu izstrādāja Informatīvo ziņojumu „Par kritērijiem kritisko informācijas un komunikācijas tehnoloģiju un informācijas sistēmu infrastruktūru noteikšanai un priekšlikumiem kiberdrošības paaugstināšanai" (turpmāk – Informatīvais ziņojums). Minētajā dokumentā tika apkopota informācija par valsts pārziņā esošo iestāžu interneta mājas lapām (turpmāk – Tīmekļa vietnēm).

Sekretariāts 2009.gadā veica situācijas analīzi Latvijā, izvērtēja 221 valsts tiešās pārvaldes iestāžu Tīmekļa vietnes pēc to informatīvajām un valsts reprezentācijas funkcijām un noteica 33 Tīmekļa vietnes, kuras satur sabiedrībai nozīmīgu informāciju un kurām jānosaka paaugstinātas drošības prasības.

Vides aizsardzības un reģionālās attīstības ministrija (turpmāk – Ministrija) pēc Sekretariāta sagatavotā Informatīvā ziņojuma pielikuma Nr.2. aktualizācijas, 25 iestādēm veica tīmekļa vietņu drošības pārbaudes. Valsts akciju sabiedrība „Latvenergo" uz Ministrijas uzaicinājumu veikt to pārziņā esošo tīmekļu vietņu drošības pārbaudi, neatsaucās. Latvijas Banka norādīja, ka regulāri veic savu Tīmekļa vietņu drošības pārbaudi, izmantojot tās rīcībā esošos drošības testēšanas rīkus un atsevišķi to pārziņā esošās Tīmekļa vietnes testēšana nav nepieciešama.

Papildus, pēc Informācijas tehnoloģiju drošības incidentu novēršanas institūcijas, Centrālā finanšu un līgumu aģentūras, Veselības inspekcijas un Valsts aģentūras „Valsts tehniskā uzraudzības aģentūra" lūguma Ministrija veica drošības pārbaudes attiecīgajām Tīmekļa vietnēm. Kopumā Ministrija no 2011.gada 18.aprīļa līdz 2011.gada 19.decembrim kopā ar atkārtotām pārbaudēm veica 54 Tīmekļa vietņu pārbaudes.

Ņemot vērā institūciju atsaucību, Ministrija arī turpmāk plāno regulāri veikt vietņu drošības pārbaudes ne tikai Ministrijām, bet arī to padotības iestāžu, kā arī pašvaldību pārziņā esošajām tīmekļa vietnēm.

~~„DIENESTA VAJADZĪBĀM"~~

NAV KLASIFICĒTS

1. Tīmekļa vietņu drošības audita veikšanas mērķis

Lai novērtētu drošības līmeni no 2011.gada 18.aprīļa līdz 2011.gada 19.decembrim Ministrija organizēja drošības pārbaudes Finanšu ministrijas, Datu valsts inspekcijas, Ekonomikas ministrijas, Izglītības un zinātnes ministrijas, Kultūras ministrijas, Korupcijas novēršanas un apkarošanas biroja, Latvijas dzelzceļa, Pilsonības un migrāciju lietu pārvaldes, Valsts robežsardzes, Tieslietu ministrijas, Valsts kases, Labklājības ministrijas, Saeimas kancelejas, Aizsardzības ministrijas, Valsts policijas, Zemkopības ministrijas, Valsts kancelejas un Ministru prezidenta, Iekšlietu ministrijas Informācijas centra, Valsts ieņēmu dienesta, Valsts ugunsdzēsības un glābšanas dienesta, Vides aizsardzības un reģionālās attīstības ministrijas, Centrālās vēlēšanu komisijas, Satiksmes ministrijas, Veselības ministrijas, Ārlietu ministrijas pārziņā esošajām Tīmekļa vietnēm.

Ņemot vērā, ka Latvijā nepastāv atsevišķs normatīvais akts un konkrēts tiesiskais regulējums, kas nosaka Tīmekļa vietņu fiziskās un loģiskās aizsardzības prasības, Ministrija veica Tīmekļu vietņu pārbaudes, lai apzinātu tajās 10[1] visbiežāk sastopamāko drošības apdraudējumu (turpmāk - ievainojamības) esamību:

1) Koda injicēšana;
2) Starpvietņu skriptēšana;
3) Nekorekti strādājošu sesiju un autentifikācijas mehānismi;
4) Nedroša tiešā atsauce uz objektu;
5) Starpvietņu pieprasījumu viltošana;
6) Nepareiza drošības konfigurācija;
7) Kriptogrāfiski nedroša datu uzglabāšana;
8) Nepilnīga URL adrešu aizsardzība;
9) Nepietiekami aizsargāts transporta slāņa līmenis;
10) Bez validācijas veiktas pāradresācijas.

Pastāvošās ievainojamības Tīmekļa vietnēs, pieļauj personu (urķu) prettiesisku iejaukšanos to darbībā un saturā, piemēram, kaitīgu programmu instalēšanu Tīmekļa vietnes darbināšanas vidē, kas dot iespēju grozīt Tīmekļa vietnes publicēto saturu, kā arī ļauj izmantot Tīmekļa vietni kā līdzekli, lai nesankcionēti izgūtu būtisku informāciju no Tīmekļa vietnes lietotājiem.

Uzbrukumu iespējas un to radītās sekas, ko šādi uzbrukumi var nodarīt Tīmekļa vietnei, ir daudzveidīgi. Tāpat dažādi var būt šādu uzbrukumu iemesli un mērķi – popularitāte, ko konkrētā sabiedrības lokā gūst urķis no tā, ka tika apietas Tīmekļa vietnes aizsardzības sistēmas, tieši vai netieši gūstamā peļņa, apzināts kaitējumus vietnes īpašnieka, izstrādātāja vai uzturētāja reputācijai, kā

[1] (https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project)

arī vietnes apmeklētāju dezinformācijas vai maldināšanas nolūkā. Nozares praksē visbiežāk izplatīti šādi uzbrukumi Tīmekļa vietnēm;

1) Galvenās (titullapas) aizstāšana – viena no visbiežāk izmantotām tehnikām, kur pierastā satura vietā tiek ievietota cita informācija – huligāniska satura vai maldīga informācija;
2) Tīmekļa vietnē uzkrātās informācijas iznīcināšana – visa informācija tiek neatgriezeniski zaudēta, gadījumā, ja nav tikusi veikta rezerves kopēšana. Finanšu iestādei tas var radīt būtiskus zaudējumus, piemēram, finanšu datu par klientiem vai citu būtisku informācijas nozaudēšanu vai noplūdi;
3) Apmeklētāju maldināšana – piemēram, Tīmekļa vietnē urķis var grozīt kontaktinformācijas sadaļā telefona numurus, lai vēlāk ar sociālās inženierijas palīdzību izkrāptu no zvanītājiem sev nepieciešamo informāciju un tādējādi vēlāk vērsties pret tiem ar ļaundabīgiem nodomiem;
4) „Trojas zirgu" izvietošana – šajā gadījumā, Tīmekļa vietņu lietotāju datori var tikt inficēti ar datorvīrusiem;
5) Mēstuļu izsūtīšana – Tīmekļa vietni var izmantot, kā mēstuļu izsūtīšanas avotu, šajā gadījumā iestādes korespondence nenonāks līdz adresātiem, jo ļoti iespējams, ka iestādes reģistrētais domēna vārds būs iekļuvis kādā no mēstuļotāju melnajiem sarakstiem;
6) Paaugstinātas slodzes radīšana – uz Tīmekļa vietni tiek nosūtīts milzīgs daudzums pieprasījumu, kā rezultātā tiek apstādināta vietnes darbināšanas vide vai tiek nopietni apgrūtināta piekļuve pie Tīmekļa vietnes resursiem.

Uzskaitītie uzbrukumu veidi ne tikai rada traucējumus Tīmekļa vietnes funkcionālai darbībai un apdraud pilnīga un nemainīta satura saglabāšanu, bet arī rada uzticamības zaudēšanu institūcijas tēlam. Ņemot vērā, ka Tīmekļa vietnē publicētai informācijai jābūt aktualizētai un patiesai, kā arī to, ka paaugstinās noziegumu attīstības tendences IT jomā, īpaša vērība ir jāpievērš Tīmekļa vietnes drošībai.

Ministru kabineta 2007.gada 6.martā noteikumi Nr.171 „Kārtība, kādā iestādes ievieto informāciju internetā" nenosaka institūcijām par pienākumu Tīmekļa vietnēm veikt regulāri pārbaudes uz ievainojamībām. Tomēr Informācijas tehnoloģiju drošības likuma 8.pantā trešās daļas 2.punktā noteikts, ka Valsts un pašvaldību institūcijām ne retāk kā reizi gadā jāveic informācijas tehnoloģiju drošības pārbaude un atbilstoši tās rezultātiem jāorganizē atklātā trūkumu novēršana. Tādējādi uz institūciju Tīmekļa vietnēm būtu jāattiecina visas tās drošības prasības, ko parasti piemēro informācijas sistēmām drošības pārvaldībā.

2. Tīmekļa vietņu drošības audita veikšanas posmi

Drošības pārbaudes laikā jāievēro priekšnoteikumi un nosacījumi, citādi definētās pārbaudes var kaitēt Tīmekļa vietnes funkcionalitātei. Tādēļ Ministrija visām institūcijām, kuras piekrita veikt Tīmekļa vietņu drošības auditu, lūdza nozīmēt laiku un datumu, kā arī atbildīgo darbinieku par Tīmekļa vietnes drošības pārvaldību.

Drošības pārbaužu rīks IBM Rational appscan 8.0 (turpmāk - Skeneris), ar ko Ministrija veica institūciju Tīmekļu vietņu pārbaudi tika iegādāts izmantojot Eiropas reģionālās attīstības fonda līdzekļus, kura pārzinis ir Valsts reģionālās attīstības aģentūra. Saskaņā ar noslēgto 2011.gada 1.aprīlī līguma Nr.6-13/11/39 starp Ministriju un Valsts reģionālās attīstības aģentūru, Skeneris tika nodots uz 3 gadiem Ministrijas lietošanai.

Tīmekļu vietņu drošības pārbaude tika veikta šādos posmos:

1) Sākotnējā informācijas apkopošana par Tīmekļa vietni. Šajā etapā tika identificēta pati Tīmekļa vietne un saturošo hipersaišu daudzums, kā arī nepieciešamo testu kopums;
2) Potenciālo ievainojamību atklāšana. Skeneris izmanto savu datu bāzi ar izplatītākām ievainojamību pazīmēm, lai audita procesā salīdzinātu tās ir iegūtiem rezultātiem;
3) Atrasto ievainojamību apstiprināšana. Skeneris izmanto speciālas metodes un modelē (imitē) noteiktus uzbrukumus uz Tīmekļa vietni, lai apstiprinātu identificēto ievainojamību eksistenci;
4) Atskaišu veidošana. Pamatojoties uz iegūtiem datiem, Skeneris izveido atskaiti, kurā ir sniegts apraksts par atklātām ievainojamībām.

3. Metodoloģija

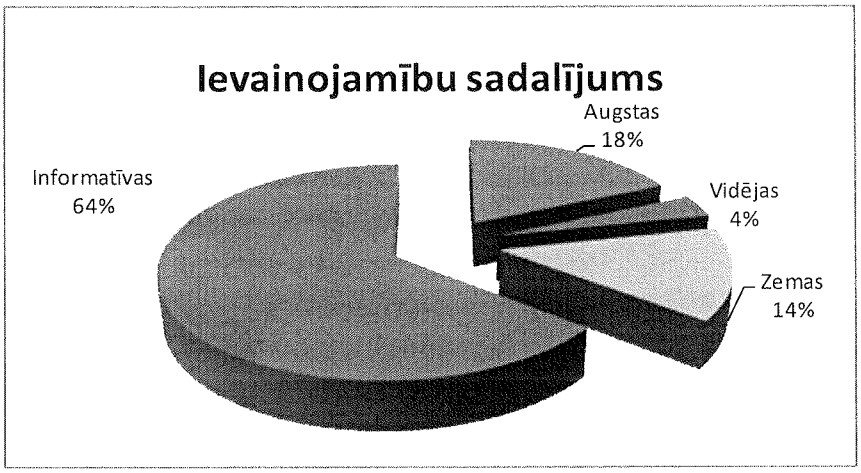
Informācija par ievainojamībām Tīmekļa vietnēs tika apkopota automātiskā drošības pārbaudes procesā bez iepriekšēju priekšdarbu veikšanas (standarta profils). Pārbaude tika veikta izmantojot „melnās kastes" principu, t.i., pārbaude, kura laikā nav zināma Tīmekļa vietnes darbināšanas vides un tās konfigurācijas īpatnības, kā arī Tīmekļa vietnes programmas kods. Identificētās ievainojamības tika iedalītas pēc būtiskuma trijās kategorijās:

1) Augsts – Liela potenciāla ietekme uz vietnes drošību vai varbūtība, ka risks īstenosies; iespējami institūcijas labā tēla zaudējumi;

2) Vidējs – Nozīmīga ietekme uz vietnes drošību vai vērā ņemama varbūtību, ka risks īstenosies; risks var realizēties kombinācijā ar citām ievainojamībām;
3) Zems – Iespējama ierobežota ietekme uz vietnes drošību. Nerada būtisku risku vietnes drošībai;

4. Statistitika par ievainojamībām

Kopumā drošības audita laikā 25 institūciju Tīmekļa vietnēs, tika identificētas 7735 ievainojamības ar dažādām ievainojamības pakāpēm, no tām 1379 augsta riska ievainojamības, kas prasa tūlītēju situācijas izvērtējumu un rīcību no institūciju puses, lai novērstu vai mazinātu potenciālo drošības apdraudējumu, kā arī 255 vidējas un 1102 zema riska informatīvās ievainojamības. Procentuāls sadalījums attēlots attēlā Nr.1.



attēls.Nr.1. Ievainojamību sadalījums pēc būtiskuma

Ministrija pēc Tīmekļa vietņu drošības pārbaužu veikšanas nosūtīja institūciju, tai skaitā Saeimas kancelejai un Centrālās vēlēšanu komisijas, atbildīgām amatpersonām par Tīmekļa vietņu drošību atskaiti par pārvaldībā esošās Tīmekļa vietnes identificētām ievainojamībām.

Veicot atkārtotas drošības pārbaudes tika secināts, ka iestādes Tīmekļa vietnēs novērsušas 32% augstas ievainojamības un 15% vidējas ievainojamības riskus. Procentuāli salīdzinoši mazais ievainojamību novēršana skaidrojama ar to, ka institūcijas Tīmekļa vietņu uzturēšanas līgumos nav paredzējušas pienākumu izstrādātājam novērst atklātās drošības ievainojamības, līdz ar to šāda pienākuma īstenošana institūcijām prasa papildus finanšu līdzekļus.

Tāpat par ievainojamību rašanās iemesliem institūciju Tīmekļa vietnēs uzskatāms:

1) Nepietiekams Tīmekļa vietnes izstrādes budžets.

Ņemot vērā ierobežotos finanšu līdzekļus, institūcijas nav varējušas piesaistīt kvalificētus drošības speciālistus, kas specificētu izstrādes prasības no drošības viedokļa.

2) Tīmekļa vietnes izstrāde nav izstrādāta atbilstoši starptautiskiem drošības standartiem.

Specificējot vietnes izstrādi, institūcijas nav norādījušas atbilstību starptautiskiem drošības standartiem, piemēram, atbilstību OWASP (Open Web Application Security Project) Tīmekļa vietņu izstrādes drošības vadlīnijām.

3) Regulāri netiek veiktas drošības pārbaudes.

Drošības pārbaudes ir nozīmīga un neatņemama vietnes drošības kontroles daļa. Regulāras pārbaudes dod iespēju novērtēt vietnes drošības stāvokli un priekšlaicīgi atklāt iespējamos apdraudējumus.

4) Tīmekļa vietņu izstrāde nav standartizēta.

Tīmekļa vietņu izstrāde ir sadrumstalota un visbiežāk balstīta uz individuāliem risinājumiem. Institūciju vietnes tiek veidotas uz atšķirīgām platformām, kā rezultātā ir ierobežotas iespējas unificēt un koplietot dažādus tehnoloģiskos risinājumus.

Papildus tika konstatēts, ka vairums institūciju Tīmekļa vietņu:

1) Neatbilst OWASP drošības prasībām kā arī nekorekti nokonfigurēta vietnes darbināšanas vide;
2) Satur failus, kurā ir sensitīva informācija par pašu vietni un tās darbināšanas vidi;
3) Produkcijas videi nav uzstādīti jaunākie programmatūras ielāpi;
4) Produkcijas vides satur trešo ražotāju programmatūru, kas rada ievainojamības;
5) Nav pienācīgi aizsargāta ar drošības infrastruktūru;

5. Ieteikumi institūciju Tīmekļa vietņu drošības uzlabošanai

Drošības pārbaudes laikā veicot risku analīzes novērtējumu un rezultātu apstrādi Ministrija sagatavoja ieteikumus, kurus ievērojot iespējams būtiski samazināt tīmekļa vietnes drošības incidentu apdraudējumu risku un nodrošināt augstāku drošības līmeni:

1) Tīmekļa vietņu izstrādes iepirkumu tehniskajā specifikācijā, institūcijām iekļaut prasību, ka izstrādātājam izstrādes/uzturēšanas laikā jānovērš vismaz OWASP 10 visizplatītākās ievainojamības;
2) Regulāri institūcijām paaugstināt Tīmekļa vietņu darbināšanas vides drošību. Novērst atklātās ievainojamības, gadījumā, ja to novēršana prasa nesamērojamus ar iespējamiem zaudējumiem finansiālos resursus, instalēt papildus drošības kontroles (piemēram, IDS, IPS, ugunsmūri utt.);
3) Regulāri valsts un pašvaldību institūcijām veikt Tīmekļa vietņu drošības pārbaudes;
4) Tīmekļa vietnes drošības pārvaldību organizēt atbilstoši Informācijas tehnoloģiju drošības likumam;
5) Institūcijām atvēlēt ik gadu no Tīmekļa vietņu uzturēšanas finanšu līdzekļiem vismaz 10% drošības paaugstināšanai.

Tīmekļa vietnes drošības uzturēšana un pārvaldība prasa noteiktus finansiālus līdzekļus un atbilstošu personālu, kā arī tehniskos resursus. Lai mazinātu iepriekš minēto faktoru ietekmi, uz Tīmekļa vietņu drošību, Ministrija kā operatīvu situācijas risinājumu piedāvā izvietot vienas nozares institūciju Tīmekļu vietnes centralizēti, atbilstoši vienota datu centra principam (Informatīvais ziņojums „Par Microsoft infrastruktūras programmatūras izmantošanas un informācijas tehnoloģiju infrastruktūras optimizācijas iespējām ministrijās un to padotības iestādēs", pieņemts zināšanai Ministru kabinetā 2010.gada 6.aprīļa sēdē (prot. Nr.17 32.§ 1.punkts).

Realizējot Tīmekļa vietņu resursu optimizāciju iespējams, būtiski uzlabot drošības līmeni Tīmekļa vietnēs. Šādas optimizācijas priekšrocības:

1) Standartizēta Tīmekļa vietņu izstrādes un darbināšanas vide;
2) Samazinātas uzturēšanas izmaksas;
3) Paaugstināta institūciju Tīmekļa vietņu satura un pakalpojumu pieejamība;
4) Paaugstināta kvalificēta tehniskā atbalsta personāla pieejamība;
5) Standartizēta drošības pārvaldība.

Saskaņā ar Informatīvo ziņojumu „Par priekšlikumiem valsts pārvaldes vietņu uzturēšanas optimizācijas iespējām", kuru Valsts Kanceleja izstrādā, balstoties uz 2010.gada 6.aprīļa Ministru kabineta sēdes protokola Nr.17 32.paragrāfa 4.punktā noteikto uzdevumu, tika secināts, ka valsts pārvalžu iestāžu Tīmekļa vietnēm izmanto 69 atšķirīgas satura vadības sistēmas, kas standartizējamo pakalpojumu resursu konsolidācijas kontekstā norāda uz optimizācijas iespējām. Tīmekļa vietņu izstrāde visbiežāk tiek balstīta uz individuāliem risinājumiem, tādējādi sadārdzinot gan izveides un uzturēšanas, gan arī tīmekļu vietņu modernizācijas jeb attīstības izmaksas. Resursu centralizācija uzlabotu līdzekļu izlietojuma efektivitāti, proti, ilgtermiņā rekomendētais risinājums ir Tīmekļa vietņu vispārējas centralizācijas virziena izvēle.

Vides aizsardzības un reģionālās attīstības ministrs E.Sprūdžs

Vīzē: Valsts sekretārs G.Puķītis

25.01.2012. 09:10
1881
J.Vašs 67770312
janis.vass@varam.gov.lv