Հավելված
ՀՀ կառավարության 2024 թվականի
սեպտեմբերի 12-ի N 1445-Լ որոշման

«Հավելված
ՀՀ կառավարության 2024 թվականի
հունիսի 14-ի N 884-Լ որոշման

ԱՄՊԱՅԻՆ ՏԻՐՈՒՅԹՈՒՄ ՏԵՂԱԿԱՅՎՈՂ ՊԱՇՏՈՆԱԿԱՆ ԿԱՅՔԵՐԻ ՆԿԱՏՄԱՄԲ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ՆՎԱԶԱԳՈՒՅՆ ՊԱՀԱՆՋՆԵՐԸ

1. ԸՆԴՀԱՆՈՒՐ ԴՐՈՒՅԹՆԵՐ

1. Սույն հավելվածով սահմանվում են ամպային տիրույթում պաշտոնական կայքերի տեղակայման անվտանգության նվազագույն պահանջները:

2. Սույն հավելվածը վերաբերում է ամպային տիրույթում տեղակայվող պաշտոնական կայքի բովանդակության ձևավորմանը և տվյալներին, տեխնիկական բաղադրիչներին, տեղեկատվական անվտանգության վերահսկմանը և մշտադիտարկմանը:

3. Պաշտոնական կայքի տեղեկատվական ռեեստրը ներառում է կայքերի վերաբերյալ հիմնական տեղեկությունները և տեխնիկական մանրամասները, որոնք առնչվում են բիզնես գործընթացների շարունակականությանը:

2. ՊԱՇՏՈՆԱԿԱՆ ԿԱՅՔԻ ԲՈՎԱՆԴԱԿՈՒԹՅԱՆ ՈՒ ՀԱՐԱԿԻՑ ՏՎՅԱԼՆԵՐԻ ԴԱՍԱԿԱՐԳՈՒՄՆ ԱՄՊԱՅԻՆ ՀՈՍԹԻՆԳՈՒՄ

4. Պաշտոնական կայքում կարող են զետեղվել միայն «հանրային» դասակարգված տեղեկությունները:

5. Օգտատերերի անձնական և նույնականացման տվյալները (մուտքանուն, գաղտնաբառ և այլն) չպետք է ցուցադրվեն կայքի որևէ հատվածում:

6. Պաշտոնական կայքի ինտերֆեյսը (interface) չպետք է պարունակի կայքերի

ստեղծման կամ կառավարման մեջ կիրառվող ամպային ծառայությունների և ծրագրային ապահովման մատակարարների վերաբերյալ գովազդային բնույթի տեղեկատվություն, բացառությամբ ներբեռնվող նյութերի:

7. Առցանց մատուցվող ծառայությունները (ոչ ստատիկ բովանդակություն, որը ստանում/պահում/մշակում է օգտատերերի տրամադրած տվյալները) պետք է տարանջատված լինեն պաշտոնական կայքի կոդից/տեխնիկական մասից:

3. ՊԱՇՏՈՆԱԿԱՆ ԿԱՅՔԻ ՏԵՂԱԿԱՅՄԱՆ, ՊԱՀՈՒՍՏԱՎՈՐՄԱՆ ԵՎ ԲԻԶՆԵՍ ՇԱՐՈՒՆԱԿԱԿԱՆՈՒԹՅԱՆ ԱՊԱՀՈՎՄԱՆ ԳՈՐԾԸՆԹԱՑՆԵՐԻ ՆԵՐԴՐՈՒՄԸ

8. Պաշտոնական կայքը պետք է տեղակայված լինի .gov.am տիրույթում (domain):

9. Պաշտոնական կայքի տեղակայման ամպային տիրույթ ընտրելիս՝ այլ հավասար պայմանների դեպքում նախապատվությունը տալ Հայաստանի Հանրապետությունում տեղակայված սերվերային ենթակառուցվածքին:

10. Ամպային տիրույթում տեղակայումը պետք է իրականացվի այնպես, որ կայքի ցանկացած թարմացում նախ կատարվի թեստավորման միջավայրում (pre-live), այնուհետև հաջող փորձարկումից հետո ապահովվի ինքնաշխատ եղանակով տեղակայումը (deployment) իրական միջավայրում (live):

11. Տեղակայման գրանցամատյանները (deployment logs) պետք է լինեն հասանելի ամպային ծառայությունների (PaaS) կամ ենթակառուցվածքի (IaaS) մակարդակով:

12. Ներդրված ցանկացած ամպային ծառայություն պետք է ներառի պաշտոնական կայքի տվյալների առնվազն օրական պահուստավորում (backup), ինչպես նաև հստակ ուղեցույցներ, թե ինչպես կարելի է վերականգնել կայքը:

13. Օրական պահուստավորումից բացի պետք է կատարվի առնվազն շաբաթական պահուստավորում (backup), ամպային ծառայությունների հիմնական մատակարարի հոսթինգից (hosting) տարբերվող վայրում (լոկալ պահուստավորում (local backup), այլընտրանքային ամպային ծառայություններ մատուցող ենթակառուցվածք):

14. Պաշտոնական կայքի ամբողջական պահուստավորման (full backup) և վերականգնման (կայքի զրոյական վիճակից) սցենարները պետք է փորձարկվեն մինչև ամպային հոսթինգում (hosting) կայքի գործարկումը:

15. Պաշտոնական կայքի ստեղծման ծրագրերը (բովանդակության կառավարման համակարգ (content management system) պետք է թարմացվեն և շտկվեն ամպային ծառայությունների մատակարարի կամ սպասարկման թիմի (DevOps) կողմից՝ ծրագրային թարմացումների առկայության դեպքում:

4. ՊԱՇՏՈՆԱԿԱՆ ԿԱՅՔԻ ՏԵԽՆԻԿԱԿԱՆ ԵՎ ԿԱԶՄԱԿԵՐՊԶԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ՊԱՀՊԱՆՄԱՆ ՄԻՋՈՑԱՌՈՒՄՆԵՐԸ

16. Պաշտոնական կայքում պետք է ներդրվեն անվտանգության ապահովման տեխնոլոգիաները (Secure Sockets Layer/Transport Layer Security-SSL/TLS):

17. Պաշտոնական կայքի ադմինիստրատորի վահանակի (admin panel) մուտքը պետք է իրականացվի երկգործոն կամ բազմագործոն նույնականացմամբ (Two-factor authentication-2FA կամ Multi-factor authentication-MFA)՝ հնարավոր դեպքերում «Ես եմ» ազգային նույնականացման հարթակի միջոցով:

18. Պաշտոնական կայքի ամպային հոսթինգի (hosting) մատակարարի ադմինիստրատորի վահանակի (admin panel) մուտքը պետք է իրականացվի երկգործոն կամ բազմագործոն նույնականացմամբ (Two-factor authentication-2FA կամ Multi-factor authentication-MFA):

19. Ցանկացած կոդ/SaaS/IaaS/PaaS արտադրանք պետք է ստեղծվի առցանց միջավայրում տեղեկատվության անվտանգության թոփ 10 (The Open Web Application Security Project-OWASP Top 10) ստանդարտներին համապատասխան:

20. Պաշտոնական կայքում խոցելիության և ներթափանցման թեստավորումը (vulnerability and penetration testing) պետք է իրականացվի նախքան դրա ուղիղ տեղակայումը (live deployment) և շարունակվի տեղակայումից հետո՝ առնվազն տարին մեկ անգամ, իսկ խնդիրների հայտնաբերման դեպքում՝ դրանք շտկել հնարավոր սեղմ ժամկետում:

21. Հնարավոր դեպքերում խոցելիության սկանավորումները, ինչպես նաև կայքի առանձին բաղադրիչների թեստավորումները պետք է ներառվեն կայքի շարունակական ինտեգրման/շարունակական տեղակայման (Continuous Integration/Continuous Deployment-CI/CD) գործընթացում:

22. Պետք է կիրառել Վեբ միջցանցային էկրան (Web Application Firewall-WAF)՝ կայքը պաշտպանելու այնպիսի վեբ հավելվածների հարձակումներից, ինչպիսիք են օրինակ՝ ԷսՔյուԷլ-ը (Structured Query Language-SQL), ԷքսԷսԷս-ը (Cross Site Scripting-XSS): Օգտագործողը պետք է հնարավորություն ունենա ստանալ հարձակումների վերաբերյալ հաշվետվությունները:

23. Ամպային ծառայությունների մատակարարը պետք է տրամադրի ԴիՕԷս (DoS) և ԴիԴիՕԷս (DDoS) հարձակումներից ավտոմատ պաշտպանություն՝ օգտատերերին տրամադրելով լրացուցիչ կանոններ սահմանելու հնարավորություն: Օգտագործողը պետք է հնարավորություն ունենա ստանալ հարձակումների վերաբերյալ հաշվետվությունները:

24. Դիտարկչի (browser) անվտանգությունն ապահովելու համար պետք է կիրառվեն այնպիսի գործիքներ, ինչպիսիք են օրինակ՝ ՍիԷսՓի-ն (Content Security Policy-CSP), ԷյչԷսԹիԷս-ը (Strict-Transport-Security-HSTS) և ԷքսՍիԹիՕ-ն (X-Content-Type-Options):

25. Ամպային հոսթինգի (hosting) մատակարարների գրանցամատյանները (application events, host-based logs և այլն) պետք է լինեն հասանելի՝ կանխելու, հայտնաբերելու և հետաքննելու հնարավոր վնասակար գործողությունները:

26. Գրանցամատյանները (logs) պետք է պահպանվեն առնվազն մեկ տարի և հասանելի լինեն ադմինիստրատորներին և Հայաստանի Հանրապետության օրենսդրությամբ նախատեսված հանրային իշխանության մարմիններին:

27. Համակարգի և ծառայությունների ադմինիստրատորների հաշիվների արտոնությունների շրջանակը պետք է լինի խիստ սահմանափակ՝ ըստ դերերի (տեխնիկական ադմինիստրատոր, բովանդակություն մշակող և այլն)՝ ապահովելով հասանելիությունը միայն անհրաժեշտ ռեսուրսներին (Role-based Access Control): Օգտատերերը պետք է հեռացվեն, երբ չունեն մուտքի կարիք:

5. ՊԱՇՏՈՆԱԿԱՆ ԿԱՅՔԻ ՊԱՐԲԵՐԱԿԱՆ ՄՇՏԱԴԻՏԱՐԿՈՒՄԸ

28. Պետք է ներդնել պաշտոնական կայքի աշխատանքի մշտադիտարկման (monitoring) գործիքներ, որոնք ծանուցում են կայքի խափանումների, հարձակումների և այլ անվտանգային խնդիրների մասին: Այս գործիքները կարող են տրամադրվել ամպային հոսթինգի (hosting) մատակարարի կողմից կամ ներդրվել պաշտոնական կայքում՝ օգտագործելով հեղինակավոր այլ մատակարարների կողմից առաջարկվող լուծումներ:

29. Ահազանգման համակարգը պետք է ծանուցումներն ուղարկի բազմաթիվ ուղիներով (ԷսԷմԷս (SMS), էլեկտրոնային փոստ, հեռախոս, ԷյՓիԱյ (API):

30. Պետք է լինի միջադեպերի արձագանքման պլան և սպասարկման համաձայնագիր (Service level agreement-SLA) պետական մարմնի, թիմի կամ այն անձանց հետ, ովքեր պատասխանատու են պաշտոնական կայքի տեխնիկական աշխատանքի համար:

31. Պաշտոնական կայքի տեխնիկական թարմացումները կամ շտկումները և դրանց հետ կապված տեխնիկական աշխատանքները պետք է պատշաճ կերպով գրանցվեն առաջադրանքների կառավարման գործիքների (task management tools) կիրառմամբ՝ համաձայնեցված պետական մարմնի, թիմի կամ այն անձանց հետ, ովքեր պատասխանատու են կայքի տեխնիկական աշխատանքի համար:

32. Պաշտոնական կայքի օգտատերերի փորձառության (User Experience) վերլուծության որևէ գործիք չպետք է հավաքի օգտատերերի անձնական տվյալները:

6. ՊԱՇՏՈՆԱԿԱՆ ԿԱՅՔԵՐԻ ՏԵՂԵԿԱՏՎԱԿԱՆ ՌԵԵՍՏՐԸ

33. Պաշտոնական կայքի տեղեկատվական ռեեստրում պետք է ներառվեն՝

1) պաշտոնական կայքի ստեղծման ծրագրերը (բովանդակության կառավարման համակարգ (content management system).

2) պաշտոնական կայքի տնօրինողի կողմից առանձին բաղադրիչների, գրադարանների և պատրաստի գործիքների օրինական օգտագործման համար

անհրաժեշտ բոլոր լիցենզիաները.

3) բաց կոդով բաղադրիչները, գրադարանները կամ գործիքները.

4) մշտադիտարկման (monitoring) գործիքների, վերլուծության, պատասխանատու թիմերի և սպասարկման համաձայնագրի (Service level agreement- SLA) հետ կապված բոլոր տեղեկությունները.

5) պաշտոնական կայքի ադմինիստրատորի վահանակի (admin panel) բոլոր օգտատերերի մասին տեղեկությունն ըստ դերերի, ներառյալ կոնտակտային տվյալները.

6) բոլոր լիցենզիաները, ամպային ծառայությունները, «ծրագրային ապահովումը որպես ծառայություն» (SaaS-Software as a Service), «ենթակառուցվածքը որպես ծառայություն» (IaaS-Infrastructure as a Service), «հարթակը որպես ծառայություն» (PaaS-Platform as a Service) լուծումները, պահուստավորման (backup) ծառայությունները և դրանց համապատասխան համաձայնագրերն ու գործողության ժամկետները.

7) պաշտոնական կայքում ներդրված անվտանգության ապահովման տեխնոլոգիաները (Secure Sockets Layer/Transport Layer Security-SSL/TLS), «SSL» հավաստագրերի պարամետրերը (թողարկող, գործողության ժամկետի ավարտ, թարմացումների ռազմավարություն և այլն).

8) պաշտոնական կայքի ամբողջական պահուստավորման (full backup) և վերականգնման (կայքի զրոյական վիճակից) սցենարների փորձարկման արդյունքները.

9) սույն հավելվածի 30-րդ կետում նշված միջադեպերի վերաբերյալ տեղեկությունը.

10) ծրագրային փոփոխությունների գրանցամատյանները (change logs) կամ սույն հավելվածի 31-րդ կետում նշված գործիքին հղումը:

7. ՊԱՇՏՈՆԱԿԱՆ ԿԱՅՔԵՐԻ ՏԵՂԱԿԱՅՄԱՆ ԱՄՊԱՅԻՆ ՏԻՐՈՒՅԹՈՒՄ ԿԱԶՄԱԿԵՐՊՈՒՄԸ

34. Պաշտոնական կայքի տվյալների ամբողջականության, հասանելիության և անվտանգության համար պատասխանատու է կայքը և տվյալները տնօրինող հանրային իշխանության մարմինը:

35. Ամպային ծառայության մատակարարի հետ պետք է ունենալ օպերատիվ կոնտակտի հնարավորություն 24/7 ռեժիմով (այդ թվում՝ ձայնային):

36. Ամպային տիրույթում պաշտոնական կայքերի տեղակայման վերահսկողությունն իրականացնում է «Կառավարության կառուցվածքի և գործունեության մասին» օրենքով սահմանված իրավասու մարմինը:

37. Ամպային տիրույթում պաշտոնական կայքերի տեղակայումից հետո դրանց նկատմամբ սույն հավելվածով սահմանվող պահանջների պահպանման և տեղեկատվական անվտանգության ապահովման աշխատանքների վերահսկողությունն իրականացնում են օրենսդրությամբ սահմանված կարգով համապատասխան վերահսկող մարմինները:

38. Պաշտոնական կայքերի տեղեկատվական ռեեստրի մշակումը, սպասարկումը և վարումն իրականացնում է «Հայաստանի տեղեկատվական համակարգերի գործակալություն» հիմնադրամը, որը հանդիսանում է նաև ռեեստրի անվտանգության պատասխանատուն:»:

ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ
ՎԱՐՉԱՊԵՏԻ ԱՇԽԱՏԱԿԱԶՄԻ
ՂԵԿԱՎԱՐ Ա. ՀԱՐՈՒԹՅՈՒՆՅԱՆ