ՀՀ տարածքային կառավարման և ենթակառուցվածքների նախարարություն

Գերմանական համագործակցություն
DEUTSCHE ZUSAMMENARBEIT

giz

Co-financed by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Agency for Development and Cooperation SDC

Տեղեկատվական անվտանգության ուղեցույց

Դավիթ Սանդուխչյան
ԻԱԿ փորձագետ

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՋԱԿՑՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

Տեղեկատվական անվտանգության համակարգը

Տեղեկատվական անվտանգության միջոցները

Տեղեկատվական անվտանգության համակարգը (ՏԱՀ) ներառում է ֆիզիկական, վարչական և տեխնիկական պաշտպանության միջոցներ (controls), ինչպես նաև տեղեկատվական անվտանգության քաղաքականությունը և աշխատանքային պլանը:

- **Ֆիզիական միջոցների** կիրառման նպատակը սարքերի, սարքավորումների, համակարգչային ցանցի ու այլ տեխնիկական միջոցների ֆիզիական անվտանգության ապահովումը:
- **Տեխնիկական միջոցների** կիրառումը ուղղված է համակարգչային ցանց մուտք գործելու, համակարգից օգտվելու հնարավորությունը սահմանափակելուն և վերահսկելուն:
- **Վարչական միջոցները** կոչված են կանոնակարգել տեղեկատվական համակարգերի օգտագործումը՝ այդ թվում ֆիզիականական և տեխնիկական միջոցների կիրառումը:

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՋԱՏՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

Տեղեկատվական անվտանգության համակարգը

Տեղեկատվական անվտանգության ստանդարտները

- Համակարգչային հարձակումներից պատշտպանված լինելու պարտրաստականությունը (տեղեկատվական անվտանգության հասունության աստիճանը - information seucirty maturity level) գնահատվում է որոշակի ստանդարտներին համապատասխանության միջոցով:
- Ամենահայտնի ու լայն կիրառում գտած ստանդրատներից է Միջազգային ստանդարտացման կազմակերպության (ՄՍԿ) կողմից մշակված և ընդունված ISO/IEC 27000 ստանդարտների շարքը (ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27701, ISO/IEC 27017, SO/IEC 27032):
- Գոյություն ունեն այլ ստանդարտներ, այդ թվում ԱՄՆ-ում մշակված NIST 800-xx շարքի ստանդարտներ և ուղեցույցներ, որոնք հիմնականում օգտագործվում են ԱՄՆ պետական համակարգերում:
- Մեծ Բրիտանիայում մշակվել են պարզեցված ստանդարտներ (Cyber Essentials), որոնք կիրառվում են փոքր և միջին բիզնեսի կողմից, կրթական ու այլ համեմատաբար փոքր կազմակերպություններում: Այն մշակվել է IASME ստանդրատի հետ համատեղ:

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՋԱՏՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

Տեղեկատվական անվտանգության համակարգը

Տեղեկատվական անվտանգության պատրաստվածությունը

- **Սկզբնական** - որոշ անվտանգության միջոցները առկա են, սակայն կիրառվում են ոչ կանոնավոր եղանակով:
- **Կրկնվող** - անվտանգության միջոցների մեծ մասը առկա է, սակայն կիրառվում է ոչ կանոնակարգված (արձագանքային) եղանակով և ավտոմատացված չեն:
- **Սահմանված** - անվտանգության միջոցները կիրառվում են ստանդարտներին համապատասխան և փաստաթղթավորված են (կանոնագարգված):
- **Կառավարվող** - անվտանգության միջոցները պրոակտիվ են, գոյություն ունի գնահատման համակարգ (մետրիկա), առկա է որոշ ավտոմատացում:
- **Կատարելագործված** - անվտանգության միջոցները ավտոմատացված են, կանխատեսելի և ներառված են գործառույթներում (ընթացակարգերում):

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՋԱՏՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

Տեղեկատվական անվտանգության համակարգը

Տեղեկատվական անվտանգության հատվածները

- Սովորաբար, սեղեկատվական անվտանգության ստանդարտներում անվտանգության միջոցները (security controls) միացնում եմ ըստ տեսակների կամ հատվածները: Օրինակ, ISO/IEC 27001 ստանդարտում 114 միջցը դասակարգված է ըստ14 խմբի (18 բաժին է բայց 14 խումբ):

- NIST 800-53 անվտանգության շրջանակը ունի 18 խումբ, որոնց մեծ մասը համընկնում է կամ օգտագործում է ISO/IEC 27001 միջոցները:

- IASME ստանդարտը, որը մշակվել է փոքր և միջին բիզնեսում և այլ համեմատաբար փոքր կազմակերպություններում: Այս ստանդարտում անվտանգության 80 միջոցը բաժանված է 8 խմբերի:

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՇԱՏՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

Տեղեկատվական անվտանգության համակարգը

Տեղեկատվական անվտանգության հատվածները (շարունակություն)

- Եթե կազմակերպությունը գտնվում է պատրաստվածություն սկզբնական փուլում, տեղեկատվական անվտանգության հատվածները կարելի է պարզեցնել և զարգանալու հետ զուգահեռ ընդլայնել՝ ըստ ստանդարտների: Որոշ հատվածներ միավորված են և զարգացման ընթացքում կարող են առանձնացվել:
  - Ենթակառուցվածքների անվտանգությունը
  - Հասանելիության և արտոնությունների կառավարումը
  - Գաղտնաբառերի կառավարման համակարգը
  - Տվյալների անվտանգությունը և գաղտնագրումը
  - Պատահարների կառավարումը և շարունակականության ապահովումը
  - Ծրագրային անվտանգությունը

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՋԱՏՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

Տեղեկատվական անվտանգության համակարգը

Գնահատման արդյունքների վերլուծությունը և զարգացման պլանը

- Յուրաքանչյուր հատվածի գնահատման արդյունքները վերլուծվում են տեղեկատվական անվտանգության միջոցների կիրառման տեսակետից:
- Սովորաբար ստանդարտների նկարագրության մեջ նշվում է եթե ոչ կոնկրետ անվտանգության միջոց, ապա առնվազն դրա ընդհանուր նկարագրությունը:
- Նույն խնդիրը կարող է լուծում ստանալ ֆիզիկական, տեխնիկական կամ վարչական միջոցների կիրառմամբ, ինչպես նաև դրանց համատեղությամբ:
- Օրինակ սերվերային սարքավորումների ֆիզիկական անվտանգությունը կարող է իրագործվել առանձացված սենյակում այն տեղակայելու, տեսադիտարկման համակարգ տեղադրելու և այնտեղ մուտք գործելու իրավունք ունեցող անձանց ցուցակը և մուտքի կանոնները հրամանով հաստատելու միջոցով:

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՋԱՏՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

Տեղեկատվական անվտանգության համակարգը

Տեղեկատվական անվտանգության համակարգի ներդնումը

- Տեղեկատվական անվտանգության գնահատումը, որի արդյունքում կազմակերպության ղեկավարը ստանում է անվտանգության հիմնական բացերի ու խոցելիությունների պատկերը:
- Բացահայտված խնդիրների դասակարգումը ըստ հրատապության աստիճանի (եթե չի կատարվել գնահատման փուլում): Խնդիրների վերլուծում լուծման եղանակների ընտրություն:
- Տեղեկատվական համակարգի բացերը լրացնելու և խոցելիությունները վերացնելու աշխատանքային պլանի նշանակում և ռեսուրսների հատկացում:
- Ոչ բոլոր բացերը և խոցելիությունները կարող են շտկվել ծախսելով համաչափ ռեսուրսներ: Եթե անվտանգության բացը հնարավոր չէ շտկել, անհրաժեշտ է մշակել հնարավոր վնասները նվազեցնելու և հետևանքները վերացնելու միջոցառումների պլան:

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՋԱՏՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

Ենթակառուցվածքների անվտանգությունը

Ենթակառուցվածքների ֆիզիկական անվտանգությունը

- Տեղեկատվական ենթակառուցվածքները ներառում եմ կազմակերպության տնօրինման ներքո գտնվող բոլոր այն համակարգչային ու ցանցային սարքավորումները, որոնք օգտագործվում են տեղեկատվության մշակման, պահպանման ու հաղորդման նպատակով:

- Սարքավորումների ու ցանցերի անվտանգության ապահովությունը ենթադրում է, որ բոլոր սարքավորումները պետք է շահագործվեն ֆիզիկապես անվտանգ պայմաններում: Դա նախ վերաբերում է գնային ու պահպանված տեղեկությունների իմաստով առավել բարձր արժեք ունեցող սերվերային սարքավորումներին:

- Համակարգչային ցանցի ֆիզիկական անվտանգությունը պետք է բացառի ցանցին ապօրինի միանալու հնարավորությունները, ինչպես նաև ցանցը ֆիզիկապես վնասելու հնարավորությունը:

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՇԱՏՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

Ենթակառուցվածքների անվտանգությունը

Ենթակառուցվածքների տեխնիկական անվտանգությունը

- Կազմակերպության բոլոր համակարգչային սարքերը, որոնք սնվում են քաղաքային էլեկտրական ցանցից, պետք է պաշտպանված լինեն հոսանքի տատանումների ու անկայուն սնուցման հետեւանքով հնարավոր վնասներից: Սովորաբար օգտագործվում են անխափան սնուցման սարքեր (ԱՍՍ):
- Ցանցի պարագիծը (network perimeter)՝ մտից ու ելից հոսքը (traffic) ապահովող տրամաբանական հատվածը՝ պետք է պարտադիր պաշտպանված լինի հրապատով (firewall) իսկ հնարավորության դեպքում նաեւ ներթափանցումների բացահայտման համակարգով (Intrusion Detection System - IDS):
- Այն դեպքերում, երբ ներքին ցանցը կազմակերպված է անլար տեխնոլոգիաների միջոցով (Wi-Fi կամ որեւէ նման այլ միջոց), այն պետք է պաշտպանված լինի գաղտնաբառով, իսկ հզորությունն ընտրվի այն աստիճանի, որպեսզի ռադիոալիքների ճառագայթումը չթափանցի կազմակերպության գրասենյակների տարածքից դուրս:

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՇԱՏՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

Ենթակառուցվածքների անվտանգությունը

Անձնական և շարժական սարքերի օգտագործումը

- Եթե աշխատակիցները ծառայողական նպատակներով օգտագործում են անձնական սարք այն պետք է պաշտպանված լինի գաղնաբառով, որը բավարարում է կազմակերպության գաղտնաբառերի հանդեպ սահմանած բոլոր պահանջներին:

- Եթե սարքն օգտագործվում է այլ անձանց կողմից՝ օրինակ, ընտանիքի անդամների, ապա իրենք պետք է օգտվեն առանձին ստեղծված պրոֆայլով (profile), որը բացառում է աշխատանքային տեղեկությունների, փաստաթղթերի ու ցանցային կարգավորումների հասանելիությունը:

- Անձնական օգտագործման հեռախոսները եւ դյուրակիր համակարգիչները (թե սեփական, թե ծառայողական) պետք է նաեւ պարտադիր գաղտնագրվեն՝ սարքը կորցնելու կամ կողոպտելու դեպքում նրանում պարունակվող տեղեկությունները պաշտպանելու նպատակով:

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՋԱՏՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

Ենթակառուցվածքների անվտանգությունը

Հեռահար աշխատանքների կազմակերպումը

- Եթե հեռահար աշխատանքները կանոնավոր բնույթ է կրում՝ անձը պետք է ունենա ստատիկ IP համար, որպեսզի այն կարողանա հատուկ գրանցել հրապատի կարգավորումներում:

- Կազմակերպության ցանցին կամ ծառայողական սերվերին միանալու դեպքում միացումը պետք է իրականացվի միայն վիրտուալ մասնավոր ցանցի ծրագրի (private virtual network client) միջոցով:

- Միացումը պետք է իրականացվի աշխատակցի սարքի ու ցանցային սերվերի միջև՝ առանց կազմակերպությանը չպատկանող կամ միջանկյալ VPN սերվերի (point-to-point VNP): Բացառություն կարող է լինեն պետական մարմինների կամ վստահված կապալառուների կողմից հատկացված միջնորդ սերվերները (trusted proxy server):

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

Ենթակառուցվածքների անվտանգությունը

Ցանցերի անվտանգութունը ըստ տեսակների

- Առավել անվտանգ են համարվում լարային ցանցերը՝ անկախ օգտագործվող տեխնոլոգիաների (օպտիկամալուսային, կոակսիալ, ամրակցված հեռախոսային):
- Նվազ պաշտպանված են համարվում շարժական կապի երկրորդ և երրորդ սերնդի G2 և G3 (GDPR, UMTS/WCDMA) ցանցերի միջոցով միացումները: Ավելի անվտանգ են չորրոդ և հինգերորդ սերնդի ցանցերը (LTE):
- WiFi և WiMax տեսակի ցանցերը համարվում են առավել խոցելի, նույնիսկ այն դեպքերում երբ դրանք պաշտպանված են գաղտնագրման միջոցով (WEP, WAP-1, WAP-2):
- Ցանկացած՝ նույնիսկ աշխատանքային ցանցի միջոցով աշխատելու դեպքում ցանկալի է օգտագործել վիրտուալ մասնավոր ցանցեր (ՎՄՑ, VPN):

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՋԱՏՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

Հասանելիության և արտոնությունների կառավարում

Հասանելիության կառավարում

- Յուրաքանչյուր աշխատակից պետք է ունենա իր անձնական ծածկագրիը (login): Անհրաժեշտ է բացառել տարբեր աշխատակիցների կողմից նույն ծածկագրի օգտագործման դեպքերը:
- Մեկ անձ կարող է ունենալ մի քանի ծածկագիր ու գաղտնաբառ, եթե դա անհրաժեշտ է տարբեր ենթահամակարգերում աշխատանքը կազմակերպելու համար:

- Աշխատանքից ազատված աշխատակցի փոխարեն ընդունված նոր աշխատակիցը պետք է ստանա իր ծածկագիրը, այլ ոչ թե ժառանգի նախորդ աշխատակցի ծածկագիրը, անգամ եթե այդ ծածկագրի գաղտնաբառը փոխվել է:
- Աշխատակիցները չպետք է թույլ տան այլ անձանց՝ այդ թվում այլ աշխատակիցների՝ օգտագործել իրենց ծածկագրերից:

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՋԱՏՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

Արտոնությունների կառավարում

- Համակարգերի հասանելիության արդյունավետ կառավարման համար խորհուրդ է տրվում նպանատիպ իրավասություններ (ոչ պարտադիր նմանատիպ աշխատանք կատարող) աշխատակիցներին միավորել ըստ խմբերի:
- Աշխատակիցների մի մասը կարող է ունենալ տվյալները փոփոխելու իրավունք, իսկ մյուսները՝ միայն կարդալու: Իրավասությունները ծավալը սահմանվում աշխատանքային պարտականություններին համապատասխան և նշվում ծառայողական հրահանգում կամ քարթում:
- Փաստաթղթերը անհրաժեշտ է դասակարգել (classification) ըստ խոհրդապայության աստիճանի ու ստանան համապատասխան պիտակ (label). Դասակարգումը եւ պիտակավորումը հնարավորություն է տալիս փաստաթուղթը ստեղծելու պահից սահմանել դրա խոհրդապահության աստիճանը եւ հասանելիության շրջանակը:

Հասանելիության և արտոնությունների կառավարում

Գաղտնաբառերի հառավարումը

- Նախընտրելի տարբերակը, որը իրագործված է ժամանակակից գրեթե բոլոր համակարգերում, դա վերջնական օգտագործողի կողմից գաղտնաբառի ընտրությունն է:
- Ժամանակ առ ժամանակ գաղտնաբառերը ցանկալի է փոխել: Դա առավել կարևոր է այն համակարգերի համար որոնք պարունակում են խորհրդապահական տեղեկատվություն:
- Համակարգչի և առանձին համակարգերի կարգավորումները պետք է լինեն այդպիսին, որպեսզի աշխատանքը որոշակի՝ սովորաբար 15 րոպեից երկար՝ դադարեցնելու դեպքում օգտատերը կրկին մուտք գործի համակարգ:
- Բարձր աստիճանի իրավասություն ունեցող օգտատերերի ծածկագրերը (օրինակ համակարգի կառավարման) գաղտնաբառերը պետք է ունենան երկու անձ:
- Համակարգի կառավարման ծածկագիրը և գաղտնաբառը պետք է լինեն նաև տնօրենի մոտ ու պահպանվեն կնքված ծրարում որևէ ապահով տեղ:

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՋԱՏՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

Տվյալների անվտանգություն

Տվյալներ տեսակները տեղեկատվական համակարգերում

- Համակարգչային տվյալները սովորաբար դասակարգում եմ երեք խմբի՝ մշակվող տվյալներ (data in use), հաղորդվող տվյալներ (data in motion կամ data in transit) և ստատիկ տվյալներ կամ տվյալներ «հանգստի վիճակում» (data in rest).

- Յուրաքանչյուր խմբի համար պետք է նախատեսվեն ու կիրառվեն համապատասխան անվտանգության միջոցներ (security controls).

- Հատուկ ուշադրություն է պետք դարձնել կենսաչափական և հատուկ կատեգորիայի տվյալների պահպանմանը և տեղափոխմանը: Այդ կատեգորիաների տվյալները պետք է պահպանել առավել բարձր անվտանգության միջոցների կիրառմամբ:

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՇԱՏՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

Տվյալների անվտանգություն

Պահպանված տվյալների անվտանգությունը

- Համակարգում «կոշտ սկավառակների» (hard drives, solid state drives) վրա խորհրդապահական՝ այդ թվում քաղաքացիների ու աշխատակիցները անձնական տվյալները՝ պետք է պահպանվեն գաղտնագրման միջոցների (ծրագրերի) կիրառմամբ:
- Որպես կանոն խորհրդապահական՝ այդ թվում անձնական տվյալներ պարունակող տեղեկությունները չպետք է պահպանվեն դյուրակիր կրաիչների վրա:
- Առանձին դեպքերում, երբ դա բխում է աշխատակցի կողմից կատարվող աշխատանքի բնույթից կարող է արվել բացառություն՝ SS կամ անվտանգության մասնագետի թույլտվությամբ:
- Կենսաչափական տվյալները էլեկտրոնային կրիչների վրա տեղափոխելիս դրանք պետք է պաշտպանված լինեն այդպես, որ կորուստի դեպքում հնարավոր չլինի կարդալ, արտահանել (extract), կրկնապատկել կամ այլ կերպ օգտագործել:

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՋԱՏՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

Տվյալների անվտանգություն

Մշակման ընթացքում գտնվող տվյալների անվտանգությունը

- Մշակման ընթացքում գտնվող տվյալների (data in use) պաշտպանությունն ապահովելու միջոցները կարող են ներառել ի լրումն տվյալների բազաներից օգտվելու լրացուցիչ գաղտնաբառ:

- Լրացուցիչ անվտանգության միջոց կարող է լինել նաև ներցանցային հրապատը, որը կապահովի բազայից օգտվել միայն համապատասխան իրավասություն ունեցող աշխատակիցների ներքին IP կամ որոշակի MAC հասցեներից (նախընտրելի տարբերակ):

- Ինչպես աշխատակցի աշխատանքային համակարգչում, այդպես էլ խորհրդապահական տվյալներ պարունակող տվյալների բազաների օգտահաշիվները պետք է ավտոմատ կերպով արգելափակվեն, եթե մուտք գործած անձը որոշակի ժամանակ որևէ գործողություն չի կատարում:

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՇԱՏՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

Տվյալների անվտանգություն

Հաղորդվող տվյալներ անվտանգությունը

- Դյուրակիր կրիչների վրա պահպանվող խորհրդապահական տվյալները պետք է պարտադիր լինեն պաշտպանված գաղտնաբառով և գաղտնագրված:

- Այն դեպքում, երբ տվյալները պետք է հաղորդվեն էլեկտրոնային հաղորդակցության միջոցներովդրանք պետք է ևս լինեն գաղտնագրված ու պաշտպանված հուսալի ալգորիտմ և բավարար երկարություն ունեցող գաղտնագրման բանալիով:

- Աշխատանքային նամակագրությունը պետք է իրականացվի միայն օգտագործելով պաշտոնական էլեկտրոնային հաղորդակցության միջոցները:

- Անձնական էլեկտրոնային փոստի օգտագործումը գործնական՝ առավել ևս խորհրդապահական տեղեկատվություն և տվյալներ հաղորդելու համար, անթույլատրելի է:

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՋԱՏՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

Անվտանգության պատահարների կառավարումը

Անվտանգության պատահարները և իրադարձությունները

Տեղեկատվական անվտանգության պատահար (information security incident) է համարվում.

- պաշտպանիչ համակարգը շրջանցելու, համակարգչային ցանց կամ համակարգ ապօրինի մուտք գործելու (այդ թվում իրավասություն չունեցող աշխատակիցների կողմից),
- համակարգի աշխատանքը խափանելու հաջողված կամ կանխված փորձը, ինչպես նաև տեղեկությունների կամ տվյալների արտահոսքը:

- Տեղեկատվական անվտանգության բոլոր պատահարները պետք է գրանցվեն, վերլուծվեն ու ստանան համապատասխան արձագանք (լուծում):
- Ոչ բոլոր համակարգչային հարձակումներն են համարվում տեղեկատվական անվտանգության պատահար: Համակարգչային հարձակումները, որոնք չեն վտանգել ցանցը կամ համակարգը ցանցի պաշտպանությունը արդյունավետ կազմակերպելու շնորհիվ, պատահար չեն համարվում: Դրանք կոչվում են անվտանգության իրադարձություն (security event):

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

Անվտանգության պատահարների կառավարումը

Անվտանգության պատահարներին արձագանքելու փուլերը

- Նախապատրաստությունը (պաշտպանության կազմակերպում):
- Պատահարների բացահայտումը և որակավորումը (պատահար է, թե իրադարձություն):
- Պատահարի լոկալիզացում (տարածման կանխումը):
- Հարձակումը վերացնելու (դադարեցման) գործողությունները:
- Համակարգի վերականգնումը և հետևանքների վերացումը:
- Վերլուծությունը և թերությունների շտկումը:

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՋԱՏՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

Անվտանգության պատահարների կառավարումը

Անվտանգության պատահարներին արձագանքելու փուլերը

- Աշխատակիցը նկատելով համակարգի ոչ կանոնավոր աշխատանքը պետք է հայտնի դրա մասին անվտանգության կամ SS մասնագետին:
- Տեղեկանալով պատահարի մասին անվտանգության (SS) մասնագետը առաջին հերթին պետք է պարզի արդյոք դա տեղեկատվական անվտանգության պատահար է, թե ոչ:
- Եթե պերզվում է, տեղի է ունենում համակարգչային հարձակում, ապա պետք է պարզել՝ այն ավատվել է, թե շարունակվեում է:

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՇԱՏՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

Անվտանգության պատահարների կառավարումը

Անվտանգության պատահարներին արձագանքելու փուլերը

- Եթե հարձակումը շարունակվում է, առաջին հերթին պետք է աշխատել կանխել պատահարը կամ նվազեցնել հետևանքները:

- Համակարգը շարքից հանելու կամ աշխատանքը խափանելու դեպքում առաջին հերթին անհրաժեշտ է կատարել վերականգնողական աշխատանքներ:

- Եթե պատահարը պարունակում է հանցագործության ակնհայտ հատկանիշներ, օրինակ՝ գաղտնի տեղեկություններ ստանալու փորձ, անհրաժեշտ է նաև հայտնել այդ մասին համապատասխան իրավապահ մարմինների:

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՋԱՏՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

Անվտանգության պատահարների կառավարումը

Անվտանգության պատահարներին արձագանքելու փուլերը

- Վտանգը կամ դրա հետ կապված հրատապ վերացման կամ նվազեցման հետ կապված գործողությունները ավարտելուց հետո անվտանգության կամ SS մասնագետը պետք է գրանցի պատահարը, նկարագրելով հնարավորինս բոլոր հանգամանքները ու հետևանքները:
- Եթե պատահարի հետևանքով տեղի է ունեցել անձնական տվյալների արտահոսք, ապա անհրաժեշտ է անհապաղ տեղադրել հայտարարություն և հայտնել այդ մասին ոստիկանություն և ՀՀ ԱՆ Անձնական տվյալների պաշտպանության լիազոր մարմնին:
- Հայտարարությունում անհրաժեշտ է նշել՝ ինչ տեսակի տեղեկությունների արտահոսք է տեղի ունեցել, երբ և ինչպես քաղաքացիները կարող են պարզել վտանգված են իրենց տվյալները, թե ոչ և ինչ է անհրաժեշտ ձեռնարկել:

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՇԱՏՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

Անվտանգության պատահարների կառավարումը

Անվտանգության պատահարներին արձագանքելու փուլերը

- Պատահարը գրանցելուց հետո անհրաժեշտ է վերլուծել այն, պարզել անվտանգության որ միջոցներն են բացակայել, սխալ կարգավորվել կամ ընտրվել, ինչպես նաև կազմել բացերը լրացնելու կամ սխալներն ուղղելու միջոցառումների պլան:
- Վերլուծության արդյունքներն ու թերությունները և բացերը վերացնելու պլանը պետք է ևս գրանցվի պատահարների մատյանում:
- Մատնայում անհրաժեշտ է նշել աշխատանքների ավարտման ժամկետները, և արդյունավետության ստուգման (գնահատման) եղանակները:
- Անվտանգության միջոցների բացերը լրացնելուց կամ ուղղելուց հետո անվտանգության կամ SS մասնագետը պետք է գրանցի աշխատանքների արդյունքները մատյանում:

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՋԱՏՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

Ծրագրային անվտանգություն

Լիցենզավորված, բաց կոդով և ոչ ստանդարտ ծրագրերը

- Անհրաժեշտ է ձգտել օգտագործել միայն լիցենզավորված համակարգեր և ծրագրեր: Առանց լիցենզիայի ծրագրեր ու համակարգեր օգտագործելը պարունակում է իրավական և տեխնիկական ռիսկեր:
- Եթե կազմակերպությունում կա չլիցենզավորված ծրագրային ապահովում, անհրաժեշտ է մշակել դրա փոխարինման պլանը: Կարելի է փոխարինել բավ կոդով անվճար կամ հին ծրագրերով, որոնք սովորաբար ավելի մատչելի են:
- Որպես կանոն, աշխատակիցները չպետք է իրավունք ունենան ինքնուրույն տեղադրել որևէ ծրագիր: Անհրաժեշտության դեպքում լրացուցիչ ծրագիր կարող է տեղադրվել կամ ներբեռնվել SS կամ SS անվտանգության մասնագետի թույլտվությամբ:
- Նախքան լրացուցիչ, ոչ ստանդարտ ծրագիր տեղադրելը կամ ներբեռնելը SS մասնագետը պարտավոր է ուսումնասիրել այդ ծրագիրը, ծանոթանալ ծրագիրը ստեղծած ընկերության վարկանիշին և այդ ծրագրի օգտագործման մասին SS հանրության արձագանքերին:

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՇԱՏՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

Ծրագրային անվտանգություն

Թարմացումը և անվտանգության կարկատների տեղադրումը

Ժամանակ առ ժամանակ կարիք է առաջանում ծրագրային ապահովման համակարգ կամ ծրագիր արդիականացնել (updating):

Արդիականացման անհրաժեշտությունը կարող է առաջանալ.

- համակարգչային տեխնիկայի փոփոխման հետևանքով,
- զարգացման ընթացքում այլ համակարգերի համատեղելիության, և պարզապես
- ծրագրի կամ համակարգի աշխատանքն ավելի արդյունավետ դարձնելու նպատակով:

Արդիականացումը հաճախ պարունակում է անվտանգության կարկատներ, որոնք ծայրահեղ կարևորն են համակարգի անվտանգությունը պահպանելու համար:

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՋԱՏՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

Ծրագրային անվտանգություն

Հակավիրուսային ծրագրել և պաշտպանիչ համակարգեր

- Համակարգչային վնասակար ծրագրերը (malware) առավել տարածված տեղեկատվական վտանգներից են:
- Յուրաքանչյուր համակարգչում է պետք է տեղադրված լինի ու շահագործվի հակավիրուսային (antivirus կամ antimalware) ծրագիր:
- Սովորաբար, աշխատանքային կայաններում (աշխատակիցների համակարգիչները) կարելի է բավարարվել անվճար հակավիրուսային ծրագրերով:
- Ցանցային ծրագրերում, ինչպիսին են էլեկտրոնային փոստի սերվերը, տվյալների բազաներ պարունակող սերվերներն ու համակարգի կենսունակության համար կարևոր հատվածները, ցանկալի է պաշտպանել վճարովի ծրագրի կիրառմամբ, որը հաճախ թարմացնում է իր հակավիրուսային բազաները:

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՇԱՏՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

Տեղեկատվական անվտանգության շարունակականությունը

- Տեղեկատվական անվտանգության ապահովումը շարունակական և անընդհատ կատարելագործվող գործընթաց է:

- SS և SS անվտանգության մասնագետները պետք է պարբերաբար ծանոթանալ համակարգչային և ցանցային նոր վտանգների մասին և մատչելի ձևով իրազեկեն աշխատակիցներին հնարավոր վտանգների ու դրանցից խուսափելու եղանակների վերաբերյալ:

- Տեղեկատվական անվտանգության աշխատանքային պլանը պետք լինի կազմակերպության գործունեության ծրագրերի մի մասը և պարբերաբար՝ առնվազն տարին մեկ անգամ, վերանայվի, շտկվի և արդիականացվի:

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՋԱՏՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

ՀՀ-ում անձնական տվյալները անվտանգության օրենսդրական պահանջները

- Հայաստանի Հանրապետության «Անձնական տվյալների պաշտպանության մասին» օրենքի 19-րդ հոդվածի 2-րդ պարբերությամբ սահմանված է, որ անձնական տվյալներ մշակողը պարտավոր է անձնական տվյալների մշակման համակարգերում օգտագործել գաղտնագրման միջոցներ:
- Օրենքը չի սահամուում օգտագործվող գաղտնագրման միջոցների ստանդարտներն ու տեսակները, լիազորելով ՀՀ կառավարությանը ընդունել անձնական տվյալների մշակման համար օգտագործվող համակարգերի հանդեպ առաջադրվող պահանջները:
- ՀՀ կառավարության «Պետական և տեղական ինքնակառավարման մարմինների կողմից էլեկտրոնային ծառայությունների մատուցման կամ գործողությունների կատարման համար օգտագործվող էլեկտրոնային համակարգերի անվտանգության, փոխգործելիության և տեխնիկական ընդհանուր պահանջները սահմանելու մասին» 31 օգոստոսի 2015 թվականի N 1093-Ն Որոշում:
- ՀՀ կառավարության «Էլեկտրոնային տեղեկատվական համակարգի միջոցով անձնական տվյալների փոխանցման կարգը հաստատելու մասին» 19 դեկտեմբերի 2019 թվականի N 1849-Ն Որոշում:

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՋԱՏՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

ՀԱՐՑԵՐ ԵՎ ՄԵԿՆԱԲԱՆՈՒԹՅՈՒՆՆԵՐ

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՋԱԿՑՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

ՀՀ տարածքային
կառավարման և
ենթակառուցվածքների
նախարարություն

Գերմանական
համագործակցություն
DEUTSCHE ZUSAMMENARBEIT

giz

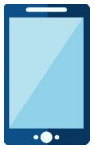
Co-financed by

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Agency for Development
and Cooperation SDC

ՇՆՈՐՀԱԿԱԼՈՒԹՅՈՒՆ

www.foi.am
www.givemeinfo.am



+374 91 407 836
+374 94 700 974

ԻՆՖՈՐՄԱՑԻԱՅԻ
ԱԶԱՏՈՒԹՅԱՆ
ԿԵՆՏՐՈՆ