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 ԱՆՎՏԱՆԳՈՒԹՅՈՒՆ

Դավիթ Սանդուխչյան
ԻԱԿ տեղեկատվական անվտանգության փորձագետ

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՉԱՏՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

ԴԱՍԸՆԹԱՑԻ ԿԱՌՈՒՑՎԱԾՔԸ

I - Տեղեկատվական անվտանգության հասկացությունը, համակարգը և միջոցները

II - Տեխնիկական միջոցների (ցանցերի և սարքավորումների) անվտանգությունը

III - Անվտանգ աշխատելաձև և վարքագիծ

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՋԱՏՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

I. Տեղեկատվական անվտանգության հասկացությունը, համակարգը և միջոցները

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՋԱՏՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

Ի՞նչ է տեղեկատվական անվտանգությունը

Տեղեկատվության անվտանգությունը ֆիզիկական, տեխնիկական և վարչական (կազմակերպչական) միջոցների համալիր է, որը կոչված է ապահովել տեղեկատվության

1. **խորհրդապահությունը**
2. **ամբողջականությունը**
3. **հասանելիությունը**

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՋԱՏՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

Տեղեկատվական անվտանգության համակարգը

Անվտանգության համակարգը ներառում է **ֆիզիկական, վարչական, և տեխնիկական պաշտպանության միջոցներ**, ինչպես նաև տեղեկատվական անվտանգության քաղաքականությունը և աշխատանքային պլանը:

Անվտանգության համակարգի կարևորագույն բաղադրիչներից է աշխատակիցների պարբերաբար ուսուցումը և նոր ի հայտ եկած տեղեկատվական վտանգների մասին շարունակական իրազեկումը:

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՋԱՏՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

Տեղեկատվական անվտանգության համար պատասխանատուները

- Կազմակերպություն բոլոր աշխատակիցները պատասխանատու են տեղեկատվական անվտանգության կանոնները պահպանելու համար:
- Կազմակերպության ղեկավարը պատասխանատու է տեղեկատվական անվտանգության համակարգը ներդնելու աշխատանքները կազմակերպելու, աշխատանքային պլանը հաստատելու և համապատասխան ռեսուրսներ հատկացնելու համար:
- Տեղեկատվական անվտանգության (տեղեկատվական տեխնոլոգիաների) գծով մասնագետը պատասխանատու է տեղեկատվական անվտանգության միջոցներ ընտրելու, առաջարկելու և փաստացի կիրառելու համար:

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՋԱՏՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

II. Տեղեկատվական անվտանգությունը աշխատավայրում

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՉԱՏՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

Տեղեկատվական անվտանգության հատվածները

- Չնայած հայտնի անվտանգության ստանդարտները պարունակում են 14-ից (ISO/IEC 27001) մինչև 32 (NIST Cybersecurity Framework) տեսակի անվտանգության միջոցներ (controls), դրանց իմացությունը հասարակ աշխատակցի համար բացարձակ անհրաժեշտ չէ:

- Ավելի պարզ, տեղեկատվական տեխնոլոգիաների ու անվտանգության ոլորտում մասնագիտական գիտելիք չունեցող աշխատակիցների համար անվտանգության միջոցները կարելի է դասակարգել ըստ երեք հիմնական խմբի.

- **Ցանցային անվտանգություն,**

- **Սարքավորումների անվտանգություն,**

- **Անվտանգ օգտագործում (անվտանգ վարքագիծ):**

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՇԱՏՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

Ցանցային անվտանգությունը

- Ցանցային անվտանգությունը, որը ներառում է անվտանգության բոլոր այն միջոցները, որոնք կոչված են արգելել կողմնակի անձանց մուտք դեպի կազմակերպության ցանց կամ համակարգ:
- Ցանցային անվտանգության միջոցները պաշտպանում են նաև տեղեկատվական համակարգում պահպանված տեղեկությունները անցանկալի արտահոսքից:
- Ցանցային անվտանգության միջոցները ի թիվս այլոց ներառում են ցանցի պարագիծը պաշտպանող սարքավորումները (հրապատ, ներթափանցման բացահայտման համակարգեր), ցանց մուտք գործելու բազմակի նույնականացման համակարգեր:

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՋԱՏՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

Ցանցերի անվտանգությունը՝ 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

Սարքավորումների անվտանգությունը

Անձնական ծառայողական համակարգչային սարքերի անվտանգության միջոցների անվտանգությունը ներառում է

- Կազմակերպությունում ներդրվող գաղտնաբառերի համակարգը ներառյալ հաղորդակցային համակարգերը (էլ. փոստ, համատեղ օգտագործման պահուստներ և սարքավորումների հասանելիություն):
- Համակարգչում պահպանված տեղեկությունների պաշտպանությունը, այդ թվում փաստաթղթերի պաշտպանությունը գաղտնաբառերի միջոցով և դրանց գաղտնագրումը:
- Խորհրդապահական տեղեկություններ պարունակող սարքերի հիշողության (պահուստների) գաղտնագրումը և ֆիզիկական պաշտպանությունը:

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՋԱՏՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

III. Անվտանգ աշխատելաձև և վարքագիծ

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՋԱՏՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

Մարդկային գործոնը

- Անվտանգ օգտագործման/վարքագծի առանձնահատկություններից մեկն է այն, որ անկախ ներդրված անվտանգության միջոցներից անվտանգությունը պայմանավորված է մարդկային գործոնով՝ յուրաքանչյուր աշխատակցի զգուշությամբ և ուշադրությամբ:
- Անվտանգության համար պատասխանատու անձանց դերը կայանում է աշխատակիցներին հնարավոր վտանգների մասին իրազեկելու և պարբերաբար անվտանգության կանոնները ստուգելու մեջ:

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՇԱՏՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

Սոցիալական ճարտարագիտությունը (social engineering)

- Հաքերային հարձակման մեծ մասը կատարվում է այդպես կոչված սոցիալական ճարտարագիտության (social engineering) միջոցով:

- Սոցիալական ճարտարագիտությունը բաղկացած է այն հնարքներից, որոնք հարձակվողը օգտագործում է իր ապագա զոհերին մոլորեցնելու և օգտվելով մոլորության տակ կատարված սխալներից մուտք գործել իրենց ցանցը, համակարգիչը, համակարգը կամ պատճառել որևէ վնաս:

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՋԱՏՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

Էլեկտրոնային նամակներ և կարճ հաղորդագրություններ

Շատ հաճախ համակարգչային (կիբեր) հարձակումները սկսվում են էլ. նամակների և/կամ հեռախոսային կարճ հաղորդագրություններ (SMS) օգտագործմամբ: Հարձակվողը կարող է ուղարկել վնասակար հղում կամ ծրագիր:

Կասկածելի նամակ ստանալու դեպքում անհրաժեշտ է.

- Համոզվել, որ նամակը ուղարկել է ձեզ հայտնի անձը իր հասցեից (ստուգել հասցեն, կարելի է զանգահարել ու ճշտել):
- Չբացել ուղարկված նամակները, կից փաստաթղթերը, նկարները, ֆայլելը մինչև չհամոզվեք, որ դրանք ուղարկել է իրական և/կամ ձեզ ծանոթ անձը:
- Չօգտագործել նամակում բերված հղումները, եթե համոզված չեք, որ դրանք ուղարկվել են իրական և/կամ ձեզ ծանոթ մարդու կողմից:

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՋԱՏՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

Գաղտնաբառերի օգտագործումը

- Հիմնականում ժամանակակից համակարգերը կառուցված են այդպես, որ համակարգը օգտագործող անձինք իրենք են որոշում իրենց գաղտնաբառը: Այսինքն գաղտնաբառը հայտնի է միայն աշխատակցին:
- Աշխատակիցները չպետք է թույլ տան այլ անձանց՝ այդ թվում այլ աշխատակիցների, օգտագործել իրենց ծածկագրերը (օգտանուններ) և գաղտնաբառերը:
- Գաղտնաբառը պետք է պարբերաբար փոխվի: Խորհրդապահական տեղեկություններ պարունակող համակերգերի գաղտնաբառերը պետք է փոփոխվեն ավելի հաճախ, օրինակ՝ երեք ամիսը մեկ անգամ:

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՋԱՏՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

Գաղտնաբառերի օգտագործումը

Գաղտնաբառը ընտրելու ժամանակ անհրաժեշտ է պահպանել որոշ կանոններ.

- Աշխատակցի (օգտատիրոջ) անունը, ապրելու վայրը (քաղաքը), ծննդյան ամսաթիվը և այլ տվյալները, որոնք կարող են հայտնի լինել երրորդ անձանց սոցիալական ցանցերի կայքերից կամ այլ բաց աղբյուրներից:
- Օգտագործել ողջամտորեն երկար (8-16 նիշ) գաղտնաբառեր, որոնք պարունակում են տառեր, թվեր և հատուկ նիշեր (օրինակ **Harza#10** կամ **adNPP$937&**):
- Չօգտագործել նույն գաղտնաբառը անձնական էլեկտրոնային փոստի օգտահաշվում (account), աշխատանքային վայրում, սոցիալական ցանցերում, բանկային համակարգում և այլ համակարգերում:

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՇԱՏՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

Տեղեկատվական անվտանգությանը հեռահար աշխատանքի դեպքում

- Հեռահար աշխատանքի դեպքում կտրուկ բարձրանում է տեղեկատվական ռիսկայնությունը: Անձը աշխատում է կազմակերպության ներքին ցանցից դուրս և հետևաբար ներքին ցանցի պաշտպանության միջոցների մի մասը չի գործում:

- Հեռահար աշխատանքի դեպքում անհրաժեշտ լրացուցիչ պաշտպանության միջոցներից է կետից-կետ մասնավոր վիրտուալ ցանցի (point-to-point VPN) օգտագործումն է և բազմակի նույնականացման համակարգերի կիրառումը:

- Առհասարակ, ՎՄՑ ցանկալի է օգտագործել բոլոր անլար ցանցին միանալու դեպքում: Նույնիսկ կազմակերպության ներքին անլար ցանցերը կարող են ունենալ անվտանգության բացեր և լինել խոցելի:

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՋԱՏՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

ՀԱՐՑԵՐ ԵՎ ՄԵԿՆԱԲԱՆՈՒԹՅՈՒՆՆԵՐ

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱԶԱՏՈՒԹՅԱՆ 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