ՀՀ տարածքային
կառավարման և
ենթակառուցվածքների
նախարարություն

Գերմանական
համագործակցություն
DEUTSCHE ZUSAMMENARBEIT

Implemented by
giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Agency for Development
and Cooperation SDC

ՏԵՂԵԿԱՏՎԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ՆԵՐՔԻՆ ՈՒՂԵՑՈՒՅՑ

տեղական ինքնակառավարման մարմինների համար

Սույն ուղեցույցը լույս է տեսնում Գերմանիայի միջազգային համագործակցության ընկերության (ԳՄՀԸ/GIZ) կողմից իրականացվող «Լավ կառավարում հանուն տեղական զարգացման Հարավային Կովկասում» ծրագրի շրջանակում՝ Գերմանիայի տնտեսական համագործակցության և զարգացման դաշնային նախարարության և Շվեյցարիայի զարգացման և համագործակցության գործակալության (ՇԶՀԳ) ցուցաբերած աջակցության շնորհիվ:

Սույն ուղեցույցի մեջ առկա տեսակետները, եզրակացությունները և պարզաբանումները անպայմանորեն չեն արտացոլում ԳՄՀԸ, ՇԶՀԳ կամ համապատասխան կառավարությունների դիրքորոշումները: Բովանդակության համար պատասխանատվությունը լիովին կրում են հեղինակները:

Հուլիս, 2021 թ.

ԻՆՖՈՐՄԱՑԻԱՅԻ ԱԶԱՏՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

Ուղեցույցը մշակվել է «Ինֆորմացիայի ազատության կենտրոն» հկ-ի կողմից

Բովանդակություն

1. Ընդհանուր դրույթներ

Սույն կանոնների նպատակն է սահմանել.

1.1 Համայնքի տեղեկատվական անվտանգության հիմնական պահանջները.

1.2 Համայնքի աշխատակազմի պարտականությունները տեղեկատվական անվտանգության պահանջների պահպանման ու վերահսկման ոլորտում.

1.3 Համայնքի գրասենյակում(գրասենյակներում) տեղեկատվական անվտանգության պահանջների ապահովման ընթացակարգերը։

2. Կանոններում օգտագործվող հասկացությունների բացատրությունը

Հաշվի առնելով, որ Կանոնակարգում օգտագործվող հիմնական հասկացությունները թարգմանվել են միջազգային ստանդարտներում օգտագործվող տերմիններից, բացատրությանը զուգահեռ բերվում են նաև անգլերեն տարբերակները։

Վնասակար (թշնամական) ծրագրեր (անգ. malware)՝ համակարգչային ծրագրեր, որոնք ստեղծվում են համակարգի աշխատանքը խափանելու, վնասելու կամ համակարգչային գրոհին աջակցելու նպատակով։

Խոցելիություն (անգ. vulnerability)՝ անվտանգության համակարգի թույլ տեղերը, բացերը, անպաշտպան հատվածները, որոնք հարձակվողը կարող է օգտագործել համակարգչային հարձակման դեպքում պաշտպանիչ միջոցները շրջանցելու, համակարգը վնասելու կամ շարքից հանելու համար։

Խոցելիության կարկատ (կամ պարզապես կարկատ, անգ. security patch)՝ համակարգի խոցելիությունը վերացնող ծրագրային լրացում։

Համակարգչային հարձակում (անգ. cyber attack)՝ համակարգչային համակարգի դեմ ուղղված գործողություններ որոնք սովորաբար ներառում են համակարգի բնականոն աշխատանքի խափանումը, համակարգում պահվող տվյալներին տիրապետելը, տվյալները ոչնչացումը, արգելափակումը կամ համակարգի օգտագործմամբ վնասակար գործողություններ կատարելը։

Հրապատ (անգ. firewall)՝ սարքավորում և/կամ ծրագրային համակարգ, որը որոշակի կանոնների համապատասխան զտում է դեպի համակարգչային ցանց մուտք գործող և/կամ ցանցից ելնող տեղեկատվական հոսքերը (տրաֆիկը)։

Պահուստային կրկնօրինակ (անգ. backup)՝ համակարգչում պահպանված տվյալների կրկնօրինակը, որը պահվում է համակարգից դուրս ու կոչված է պահպանելու տվյալների անվտանգությունն այն դեպքերում, երբ հիմնական կրիչների վրա դրանք ոչնչացվել կամ անհասանելի են դարձել։

Անվտանգության վերահսկման միջոցներ կամ անվտանգության միջոցներ (security controls)՝ տեխնիկական, ներառյալ՝ ծրագրային միջոցներ, ֆիզիկական պաշտպանության գործիքներ ու կանոններ (վարչական միջոցներ), որոնք կոչված են նվազեցնելու համակարգչային գրոհների ռիսկերը և մեղմացնեն դրանց հետևանքները։

3. Տեղեկատվական անվտանգության համար պատասխանատուները

Կազմակերպության յուրաքանչյուր աշխատակից պատասխանատու է տեղեկատվական անվտանգության ապահովման համար: Այնուամենայնիվ, յուրաքանչյուր կազմակերպություն պետք է ունենա տեղեկատվական անվտանգության համակարգը ներդնելու, պահպանելու ու արդիականացնելու համար պատասխանատու անձ:

Տեղեկատվական անվտանգության համար առաջին հերթին պատասխանատու է կազմակերպության ղեկավարը՝ սահմանելով տեղեկատվական անվտանգության ապահովումը որպես խնդիր, հանձնարարելով մշակել համապատասխան ներքին կանոնակարգեր (կանոններ, ընթացակարգեր) և ապահովելով դրանց կիրառումը:

Կազմակերպության տեղեկատվական անվտանգության անմիջական ապահովման պարտականությունը կրում է տեղեկատվական տեխնոլոգիաների մասնագետը: Տեղեկատվական տեխնոլոգիաների գծով մասնագետը պետք է ապահովի անվտանգության վերահսկման միջոցների առկայությունը ու պարբերաբար անցկացնի այդ միջոցների ստուգման միջոցառումները:

Տեղեկատվական անվտանգության անկախ ու անկողմնակալ գնահատում ու անվտանգության միջոցների վերաբերյալ առաջարկներ ներկայացնելու նպատակով կազմակերպությունը՝ տեղեկատվական անվտանգության մասնագետի առաջարկով՝ կարող է պայմանագրային հիմունքներով ներգրավվել տեղեկատվական անվտանգության մասնագետ կամ մասնագիտացված ընկերություն:

4. Տեղեկատվական անվտագնության համակարգը

Տեղեկատվական անվտանգության համակարգը (ՏԱՀ) ներառնում է տեխնիկական, ֆիզիկական ու վարչական միջոցներ, որոնք կոչված են ապահովել կազմակերպության տեղեկատվական անվտանգությունը: Տեղեկատվական անվտանգության տակ հասկանում ենք կազմակերպության համար արժեքավոր տեղեկատվության խորհրդապահության, ամբողջականության ու հասանելիության ապահովումը:

Խորհրդապահության ապահովումը նշանակում է, որ յուրաքանչյուր տեղեկատվություն հասանելի է միայն համապատասխան իրավասություն ունեցող անձանց: Խոհրդապահության ապահովման հիմնական միջոցներն են հասանելիության կառավարման համակարգը (access managment system), գաղտնաբառերի կառավարման կանոնները (password managment rules) և գաղտնագրման կանոնները:

Տեղեկատվության ամբողջականությունը նշանակում է, որ այն չի փոփոխվում և չի ոչընչացվում առանց նման գործողություններ կատարելու իրավասություն ունեցող անցի իմացության կամ թույլտվության: Անվտանգության այդ բաղադրիչը ևս ապահովվում է հասանելիության կառավարման համակարգի, գաղտնաբառերի կառավարման կանոնների ու անհրաժեշտության դեպքում նաև գաղտնագրաման կանոնների կիրառման միջոցով:

Տեղեկատվության հասանելիությունը նշանակում է, որ կազմակերպության աշխատակիցներին տեղեկատվությունը հասանելի է այն ժամանակ, երբ իրենք իրավասու են օգտվել այդ տեղեկատվությունից (աշխատանքային ժամերին, եթե աշխատանքային պարտականությունները չեն նախատեսում շուրջօրյա մուտքի իրավունք): Տեղեկատվության հասանելիությունն ապահովվում է սարքերի ու կրիչների ֆիզիկական ու ցանցային

անվտանգությունը ապահովելու, վթարային իրավիճակներին արձագանքելու և վթարների կամ հարձակումների հետևանքով համակարգի աշխատանքի խափանումները վերականգնելու համար նախատեսված միջոցառումների պլանավորմամբ ու փորձարկմամբ:

Տեղեկատվական համակարգը պետք է պարբերաբար՝ առնվազն տարին մեկ անգամ, վերանայվի կազմակերպության պատասխանատու անձանց կողմից: Վերանայումը սովորաբար կազմակերպում է ղեկավարը, անցկացնում SS մասնագետը (անվտանգության մասնագետի առկայության դեպքում նաև նրա մասնակցությամբ):

Տեղեկատվական անվտանգության կատարելագործման գործիքներից մեկը պարբերաբար անցկացվող արտաքին ստուգումներն են: Ստուգումը կարող է իրականացվել կողմնակի անկախ անվտանգության մասնագետի կամ մասնագիտացված կազմակերպության կողմից: Պետական համապատասխան անվտանգության ծառայության առկայության դեպքում պետական, տեղական ինքնակառավարման կամ հանրային կառույցներում տեղեկատվական գնահատականը կարող է անցկացվել նման ծառայության կամ հաստատության կողմից:

5. Ենթակառուցվածքի անվտանգությունը

5.1. Ֆիզիկական անվտանգության կանոնները

Տեղեկատվական ենթակառուցվածքները ներառում եմ կազմակերպության տնօրինման ներքո գտնվող բոլոր այն համակարգչային ու ցանցային սարքավորումները (համակարգիչներ, ուղղորդող սարքեր) համակարգչային ու հեռահաղորդակցային ցանցերը, որոնք օգտագործվում են տեղեկատվության մշակման, պահպանման ու հաղորդման նպատակով: Ժամանակակից տեղեկատվական համակարգերը ներառում են նաև այդպես կոչված տեղեկատվական ամպային պահուստներում (cloud storage), որոնց օգտագործումը օրեցօր աճում է ու զարգանում՝ փոխարինելով նյութական կրիչները:

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:

Սերվերային սարքավորումը պետք է պահպանվի առանձին սենյակներում (սերվերային սենյակ), որոնք պետք է հագեցած լինեն օդափոխիչներով, հակահրդեհային, իսկ հնարավորության դեպքում՝ նաև պահպանության համակարգով: Ընդ որում, հակահրդեհային համակարգը պետք է ընտրվի այնպես, որ դրա աշխատանքը չվնասի սերվերային սարքավորումներին: Ջրային հակահրդեհային համակարգերի օգտագործումն արգելվում է, քանի որ ջուրը մեծ հավանականությամբ կվնասի սարքավորումներին՝ շարքից հանելով նաև տեղեկատության կրիչները:

Սերվերային սենյակներ մուտք գործելու իրավունք պետք է ունենան միայն այն աշխատակիցները (սովորաբար համակարգի կառավարիչը - system adminsitrator), որոնք պատասխանատու են սերվերային սարքավորման սպասարկման ու վերանորոգման համար, ինչպես նաև իրենց կողմից լիազորված սպասարկող կապալառուների ներկայացուցիչները: Սերվերային սարքավորումների վրա սպասարկման, վերանորոգման կամ վերականգնման աշխատանքներ կատարելիս համակարգի կարգավորողը պետք է

գրառում կատարի այդ նպատակների համար հատուկ վարվող սպասարկման մատյանում՝ նկարագրելով կատարված աշխատանքները ու կատարողների անունները։

Համակարգչային ցանցի ֆիզիկական անվտանգությունը պետք է բացառի ցանցին ապօրինի միանալու հնարավորությունները, ինչպես նաև ցանցը ֆիզիկապես վնասելու հնարավորությունը։ Ցանցի մալուխները պետք է անցկացվեն կազմակերպության տարածքում, իսկ եթե դա անհնար է կամ տեխնիկապես բարդ, ապա պետք է պաշտպանված լինեն արտաքին միջավայրի ազդեցությունից և ներթափանցման հնարավորությունից, օրինակ՝ կարող են պաշտպանված լինել մետաղյալ ծածկատուփով։

5.2. 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), որոնք ունեն նաև էլեկտրական հոսանքի տատանումներն հարթելու հնարավորություն (Line-interractive UPS)։ Սերվերային սարքավորումները ու ցանցային ուղղորդող սարքերը գերադասելի է ապահովել մեծ ունակություն ունեցող ԱՍՍ-ով։

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։ Գաղտնաբառերի կառավարման կանոնների սկզբունքները առանձին ներկայացված են սույն ուղեցույցի համապատասխան բաժնում։

Այն դեպքում երբ կազմակերպության անլար (ռադիո) ցանցը օգտագործվում է նաև քաղաքացիներին կամ այցելուներին դեպի համացանց կամ կազմակերպության կայք էջ մուտք ապահովելու նպատակով, անհրաժեշտ է օգտագործել ոչ միայն առանձին անլար ուղղորդիչ սարք (wirless router), նաև տարանջատել ներքին ու հյուրերին հասանելի ցանցերը։

Որպես ցանցային անվտանգության գործիք հաճախ կիրառվում են այդպես կոչված «մեղր ամաններ» (honey pot)՝ կեղծ համակարգչային կայաններ, բազաներ և տեղեկություններ, որոնք կարող են դառնալ հարձակվողների համար գրավիչ թիրախ, բացահայտեն հարձակումները և չեզոքացնեն դրանք մինչև արժեքավոր հատվածներ հասնելը։ Նման համակարգերը սովորաբար տեղադրվում են այդպես կոչված «ապառազմականացված» գոտիներում (demilitarized zone կամ DMZ)։

5.3. Անձնական սարքեր, շարժական և հեռավար աշխատանքներ

Որպես կանոն, անձնական օգտագործման սարքերի՝ դյուրակիր համակարգիչների (laptops, notebooks, netbooks), շարժական կապի հեռախոսների ու պլանշետների (tablets)՝

օգտագործումը աշխատանքի համար չպետք է թյուլատրվի: Աշխատանքի համար անձնական սարքերի օգտագործման տակ հասկանում ենք սարքերում ծառայողական փաստաթղթեր մշակելը, պահպանումը, կամ այդ սարքերի օգտագործմամբ ներքին ցանց՝ առավել ևս տվյալների բազաներ՝ մուտք գործելը:

Միևնույն ժամանակ, ժամանակակից աշխատանքային պայմանները ենթադրում են աշխատանքային ընթացակարգերի թվայնացում, որն անհնար է առանց շարժական սարքերի լայն օգտագործման: Եթե կազմակերպությունը շարժական սարքի օգտագործման անհրաժեշտություն ունի, ցանկալի է որպեսզի սարքերը լինեն ծառայողական և օգտագործվեն ընդունված անվտանգության նորմերին համապատասխան:

Սակայն, ոչ բոլոր ՏԻՄ-երը կարող են հատկացնել իրենց աշխատակիցներին ծառայողական սարքեր, և աշխատակիցներն շատ անգամ օգտագործում են իրենց սեփական շարժական հեռախոսները, դյուրակիր համակարգիչներն ու պլանշետները: Նման պրակտիկան ընդունելի է որոշ վերապահումներով և որոշակի պայմանների ներքո:

ա) Առաջին ու առավել կարևոր պայմանը անվտանգության կանոնների պահպանումն է: Անձնական սարք մուտքը պետք է պաշտպանված լինի գաղնաբառով, որը բավարարում է կազմակերպության գաղտնաբառերի հանդեպ սահմանած բոլոր պահանջներին (մանրամասները տես՝ ուղեցույցի համապատասխան բաժնում):

բ) 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: Պրոֆայլի կարգավորումները պետք է ստուգվի կազմակերպության SS անվտանգության պատասխանատու անձի կողմից:

գ) Բացի մուտք գործելու համար գաղտնաբառ օգտագործելուց, 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:

դ) Հեռահար աշխատանքի դեպքում՝ եթե նման աշխատանքը 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: Ընդ որում, միացումը պետք է իրականացվի աշխատակցի սարքի ու ցանցային սերվերի միջև՝ առանց կազմակերպությանը չպատկանող կամ միջանկյալ VPN սերվերի: Բացառություն կարող է լինեն պետական մարմինների կամ վստահված կապալառուների կողմից հատկացված միջնորդ սերվերները (proxy server):

6. Հասանելիության և արտոնությունների կառավարում

Դեպի կազմակերպության տեղեկատվական համակարգ ցանկացած մուտքը պետք է հասանելի լինի միայն կազմակերպությաուն աշխատակիցների համար: Բացառիկ դեպքերում համակարգ կարող են մուտք գործել կապալառուները և համակարգը սպասարկող կազմակերպությունները, որոնց գործողությունները պետք է վերահսկվեն կազմակեր-

պության պատասխանատու անձի կողմից, սովորաբար SS մասնագետի կամ համակարգը տնօրինող մասնագետի (system administrator)։ Բոլոր աշխատակիցները մուտքը պետք է լինի միայն գաղտնագրով պաշտպանված համակարգի միջոցով (password proted access)։

Յուրաքանչյուր աշխատակից պետք է ունենա իր անձնական ծածկագրիը (logiո)։ 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։ Օրինակ, եթե կազմակերպությունը սպասարկում է փոխկապակցված կազմակերպությունների բազաներ կամ վարում է այլ կազմակերպությունների տվյալների բազաներ։ Օրինակ, տեղական ինքնակառավարման մարմինները կարող են մուտք ունենալ պետական կառավարման մարմինների բազաներ կամ հակառակը՝ վարել բազաներ, որոնցից կարող են օգտվել այլ ՏԻՄ-եր ու պետական կազմակերպություններ։

Ծածկագրերը չպետք է փոխանցվեն մեկ աշխատակցից մյուսին։ Օրինակ, եթե որևէ աշխատակցի պաշտոնը փոխվել է, անհրաժեշտ է փոխել ոչ թե նրա ծածկագիրը, այլ նրա, որպես օգտատեր իրավասությունների ծավալը։ 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։

Տեղեկատվական բազաները, թվային թղթապանակները (files folders) և բուն փաստաթղթերը պետք է հասանելի լինեն միայն այն աշխատակիցներին, որոնց պարտականությունները նախատեսում են տվյալ տվյալների բազաների կամ փաստաթղթերի հետ աշխատանքային պարտականություններ։ Օրինակ, ֆինանսական բնույթի բազաները / ծրագրերը, հաշվետվությունները ու առանձին տեսակի փաստաթղթերը, օրինակ՝ աշխատավարձերի ցուցակը, պետք է հասանելի լինեն կազմակերպության հաշվապահությանը և ֆինանսական այլ ծառայություններին, որոնց ամենօրյա աշխատանքի համար անհրաժեշտ է նման տեղեկատվությունը։

Համակարգերի հասանելիության արդյունավետ կառավարման համար խորհուրդ է տրվում նպանատիպ իրավասություններ (ոչ պարտադիր նմանատիպ աշխատանք կատարող) աշխատակիցներին միավորել ըստ խմբերի։ Ցանցերը սպասարկող գրեթե բոլոր ցանցային համակարգերը (Microsoft Active Directory for Windows serer, Group Policy Objective for open source servers) հնարավորություն ունեն խմբավորել օգտատերերին ըստ հասանելիության իրավունքների։ Օրինակ, բոլոր օգտատերերը, ովքեր լիազորված են աշխատել անձնական տվյալների բազաների հետ, կարող են միավորվել մեկ առանձին խմբի մեջ։ Ընդ որում, նրանց մի մասը կարող է ունենալ տվյալները փոփոխելու իրավունք, իսկ մյուսները՝ միայն կարդալու։

Տեղեկատվական անվտանգության միջազգային (օրինակ ISO 27001 կամ NIST 800-30) փաստաթղթերը պետք է դասակարգվեն (classification) ըստ խոհրդապայության աստիճանի ու ստանան համապատասխան պիտակ (label). Դասակարգման ու պիտակավորման հնարավորություն ունեն գրեթե բոլոր տեքստային խմբագրման ծրագրերը, այդ թվում՝ լայն տարածված Microsoft Word ծրագիրը։ Դասակարգումը և պիտակավորումը հնարավորություն է տալիս փաստաթուղթը ստեղծելու պահից սահմանել դրա խոհրդապահության աստիճանը և հասանելիության շրջանակը։

Հասանելիությունը որոշելիս պետք է ղեկավարվել այդպես կոչված «նվազագույն արտոնությունների» սկզբունքով, որը նշանակում է որ ցանկացած օգտատեր պետք է ունենա նվազագույն հասանելիություն ու գործողություններ կատարելու հնարավորություն, որն անհրաժեշտ է իրենց պարտականությունները կատարելու համար: Հասանելիության կամ գործողություն կատարելու իրավասությունը պետք է որոշվի աշխատակցի (ծածկագրի օգտատիրոջ) պարտականությունների շրջանակով՝ ըստ պաշտոնական հրահանգի, ծառայողական անձնագրի (քարթի), աշխատանքային կամ ծառայություններ մատուցելու պայմանագրի:

Պարտավորությունների շրջանակը սովորաբար որոշում է մարդկային ռեսուրսների, կադրերի ղեկավարման կամ նման այլ ստորաբաժանումը/մասնագետը, որը հաստատում է կազմակերպության ղեկավարը: Այն դեպքում երբ կազմակերպությունում ընդունված է և գործում է կադրային կանոնակարգ, այն պետք է ներառի համապատասխան ընթացակարգ: Հակառակ դեպքում կազմակերպության աշխատակիցները կարող են ղեկավարվել համակարգչային կանոններով կամ ուղեցույցերով:

Ժամանակ առ ժամանակ, ցանկալի է եռամսյակը մեկ, սակայն ոչ պակաս քան տարեկան երկու անգամ, համակարգը տնօրինողը (sytem administrator) տեղեկատվական տեխնոլոգիաների մասնագետի ու մարդկային ռեսուրսները կառավարող ստորաբաժանման կամ մասնագետի հետ միասին պետք է անցկացնեն իրավասությունների ստուգում ու վերանայում: Ստուգման նպատակը պետք է լինի իրավասությունները ու աշխատակիցների պարտականությունների համապատասխանության հաստատումը:

Որպես կանոն, խորհրդապահական տեղեկատվություն՝ այդ թվում անձնական տվյալներ պարունակող համակարգերի հասանելիությունը պետք է սահմանափակ լինի աշխատանքային օրերով ու ժամերով: Առանձին դեպքերում աշխատակիցները կարող են ստանալ ոչ աշխատանքային ժամերին կամ օրերին այդ համակարգեր մուտք գործելու իրավունք, սակայն միայն այն դեպքում, երբ համակարգի անվտանգությունը լինի համակարգը տնօրինողի կամ անվտանգության մասնագետի վերահսկողության տակ:

Հասանելիության հետ կապված ցանկացած գործողություններ, օրինակ՝ ցանց կամ համակարգ մուտքն ու ելքը գործելը, տվյալների բազաներում տվյալներ լրացնելը, փոփոխելը, ոչնչացնելը՝ պետք է գրանցվեն էլեկտրոնային համապատասխան ռեեստրներում (log registers): Ռեեստրները պետք է պարբերաբար ստուգվեն SS մասնագետի կամ SS անվտանգության մասնագետի կողմից: Ստուգումները կարող են կատարվել ըստ չափանիշների (մուտքի ու ելքի միջին քանակը, աշխատանքային ժամերի սահմանները և այն): Ստուգելի արդյունքները պետք է գրանցվեն ստուգման մատյանում նշելով ստուգողի անունը, ամսաթիվը, ստուգման ծավալը և արդյունքները: Ստուգման նպատակը պետք է լինի անկանոն կամ տարօրինակ գրանցումները կամ մուտքերը: Տարօրինակ գործողություն կարող է համարվել ոչ աշխատանքային ժամերին մուտքերը կամ սովորականից ավել ակտիվ մուտքերը:

7. Գաղտնաբառերի կառավարում

Գաղտնաբառերի կառավարման համակարգը ցանցային ու հասանելիության անվտանգության առանցքային մեջոցներից է: Համակարգը ամբողջությամբ կառավարվում է համակարգը տնօրինողի կողմից (system administrator):

Գաղտնաբառերը պետք է բավարարեն առնվազն հետևյալ պահանջներին.

ա) Կազմված լինեն ութից ավել նիշերից, պարտադիր ներառեն մեծ ու փոքր տառեր, թվեր ու հատուկ նիշեր (տոկոսի նշան, վանդականիշ, աստղանիշ և այլն)։

բ) Չպարունակեն աշխատակցի անձնական տվյալները (անունը, ազգանունը, ծննդյան թիվը) ու առհասարակ որևէ բառ կամ պատմական տարեթիվ։

Սկզբնական՝ աշխատակցին առաջին անգամ դեպի կազմակերպության ցանց մուտքի իրավունք ստանալու համար գեներացված գաղտնաբառը պետք է փոխանցվի աշխատակցին անձամբ կամ հաղորդվի հուսալի կապի միջոցով (օրինակ՝ զանգահարելով նրա անձնական հառախոսին)։ Սկզբնական գաղտնաբառը պետք է օգտագործվի աշխատակցի կողմից մեկ անգամ՝ իր գաղտնաբառը ստեղծելու համար, որը պետք է իմանա միայն ինքը՝ աշխատակիցը։ Գաղտնաբառը մոռանալու դեպքում աշխատակիցը պետք է դիմի համակարգի տնօրենին և ստանալով նոր սկզբնական գաղտնաբառ՝ նույն ընթացակարգով ստեղծի նոր գաղտնաբառ։

Կազմակերպության կողմից կամ կազմակերպության համար վերջինիս պատվերով ստեղծված ծրագրերում (սեփական ծրագրեր կամ համկարգեր) գաղտնաբառերի կառավարման համակարգերը պետք է համապատասխանեն նույն պահանջներին, ինչ ընդունված են կազմակերությունում արդյունաբերական (market available software) ծրագրերի դեպքում։ Սեփական ծրագրերի ու համակարգերի մեջ հատուկ ուշադրություն է պետք դառնձնել գաղտնաբառերի պահպանման հարցերին Սեփական ծրագրերում ու համակարգում գաղտնաբառերի ստուգման համար պետք է օգտագործվեն ոչ թե ծածկագիրի ու գաղտնաբառի համապատասխանությունը, այլ դրանց հեշ ֆունկցիայի (արտադրյալին) համապատասխանությունը, կամ գաղտնագրման որևէ այլ եղանակի կիրառմամբ։

Գաղտնաբառները, որոնք արտահոսվել են կամ որևէ այլ կերպ հայտնի են դարձել այլ անձանց, պետք է փոփոխվեն անմիջապես։ Ընդ որում, արտահոսքի մասին տեղեկանալու պահից համակարգը պետք է փակվի բոլոր օգտատերերի համար՝ բացառությամբ համակարգի տնօրենի կամ համակարգը սպասարկող կապալառու կազմակերպության կոնկրետ անձի։

Ժամանակ առ ժամանակ գաղտնաբառերը ցանկալի է փոխել։ Դա առավել կարևոր է այն համակարգերի համար որոնք պարունակում են խորհրդապահական տեղեկատվություն։ Որպես կանոն, խորհրդապահական տեղեկատվություն, այդ թվում անձնական տվյալներ, ծառայողական գաղտնիք կամ ներքին շրջանառության փաստաթղթեր կամ տեղեկություններ պարունակող համակարգերում գաղտնաբառերը պետք է փոխվեն յուրաքանչյուր 60 օր անց, մնացած՝ ոչ խորհրդապահական համակարգերում՝ 90 օրը մեկ։

Համակարգչի և առանձին համակարգերի կարգավորումները պետք է լինեն այդպիսին, որպեսզի աշխատանքը որոշակի՝ սովորաբար 15 րոպեից երկար՝ դադարեցնելու դեպքում օգտատերը կրկին մուտք գործի համակարգ։ Երկար ժամանակ՝ օրինակ սովորաբար ամենամյա արձակուրդի տևողությունից ավել՝ չօգտագործվող օգտահաշիվները արգելափակվեն ավտոմատ կերպով ու աշխատանքի աշխատատեղ վերադառնալիս նորից ստանա սկզբնական գաղտնաբար և ստեղծի նորը, ինչպես նկարագրված է ուղեցույցի համապատասխան բաժնում։

Հատուկ ուշադրություն է պետք դարձնել համակարգի տնօրինման (system administration), անվտանգության վերահսկողության (security administration) և այլ լայն իրավասություններ իրականացնող անձանց գաղտնաբառերի նկատմամբ։ Բարձր աստիճանի իրավասություն ունեցող օգտատերերի ծածկագրերը ու գաղտնաբառերը պետք է ունենան երկու անձ։ Համակարգի կառավարման ծածկագիրը և գաղտնաբառը պետք է լինեն նաև

տնօրենի մոտ ու պահպանվեն կնքված ծրարում որևէ ապահով տեղ, որը հասանելի լինի կազմակերպության ղեկավարին ու նաև անվտանգության մասնագետին, եթե կազմակերպությունը ունի նման մասնագետի հաստիք:

8. Տվյալների անվտանգություն

Տվյալների անվտանգությունը ներառում է տեխնիկական, վարչական և ֆիզիկական միջոցառումների համալիր, որն ապահովում է տեղեկատվական համակարգում պահպանված, հաղորդվող ու մշակվող բոլոր արժեքավոր տվյալների խորհրդապահությունը, ամբողջականությունը և հասանելիությունը: Տեղեկատվական անվտանգության այս երեք բաղադրիչը պետք է միշտ հաշվի առնվի ցանկացած անվտանգության միջոց մշակելիս: 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: 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:

Պետության կողմից կարող են սահմանվել անձնական տվյալներ մշակող էլեկտրոնային համակարգերի ստանդարտներ: Անձնական տվյալներ մշակողը՝ սահմանված ստանդարտային կամ չափանիշներին համապատասխանելու դեպքում՝ կարող է դիմել անձնական տվյալների անձնական տվյալները պաշտպանության մարմնին՝ բավարար պաշտպանության մակարդակ ունեցող կազմակերպությունների ռեեստրում ընդգրկվելու խնդրանքով:

8.1. Պահպանված տվյալները (data in rest)

Համակարգում «կոշտ սկավառակների» (hard drives, solid state drives) վրա խորհրդապահական՝ այդ թվում քաղաքացիների ու աշխատակիցները անձնական տվյալները՝ պետք է պահպանվեն գաղտնագրման միջոցների (ծրագրերի) կիրառմամբ: Գաղտնագրման միջոցները (ծրագրերի կիրառումը) ապահովում է տվյալների անվտանգությունը դրանց արտահոսքի կամ ցանց (համակարգ) այլ անձանց ապօրինի ներթափանցման դեպքերում: Դյուրակիր կրիքների (USB, CD-ROM, արտաքին «կոշտ սկավառակներ») վրա խորհրդապահական տեղեկատվություն կամ տվյալներ պահպանելու դեպքում դրանց ևս պետք է գաղտնագրվեն, պահպանվեն գաղտնաբառով և պահվեն ապահով տեղերում՝ կողպված պահարաններում և սենյակներում:

Որպես կանոն խորհրդապահական՝ այդ թվում աձնական տվյալներ պարունակող տեղեկությունները չպետք է պահպանվեն դյուրակիր կրիչների վրա: Առանձին դեպքերում, երբ դա բխում է աշխատակցի կողմից կատարվող աշխատանքի բնույթից կարող է արվել բացառություն՝ SS կամ անվտանգության մասնագետի թույլտվությամբ: Դյուրակիր

սարքավորումների հիշողությունը պետք է լինի գաղտնագրված և պաշտպանված սույն ուղեցույցի պահանջներին համապատասխանող գաղտնաբառով: Ցանկացած դեպքում, դյուրակիր, մանավանդ անձնական սարքավորումներում խորհրդապահական տեղեկությունները և տվյալների պահպանումը թույլատրվում է միայն SS կամ անվտանգության կողմից բոլոր անվտանգության միջոցների կիրառումը ստուգելուց հետո:

Նույնիսկ լավագույն անվտանգության համակարգերը կարող են ունենալ բացեր: Տվյալների պաշտպանության պարտադիր մաս է կազմում տվյալների պահուստային պատճեներ ստեղծելը ու դրանք պարբերաբար թարմացնելը: Նախընտրելի պարբերականությունը ամենօրյա թարմացումն է, սակայն ֆինանսական կամ տեխնիկական ռեսուրսների բացակայության դեպքում շաբաթական թարմացումը կարող է համարվել բավարար: Կայուն (ստատիկ) բազաների համար նույնիսկ ամսական պահուստավորումը կարող է լինել բավարար: Ցանկացած դեպքում պահուստավորման պարբերականությունը պետք է որոշի SS մասնագետը, իսկ տեղեկատվական անվտանգության մասնագետ ունեցող կազմակերպություններում նաև նրա մասնակցությամբ:

Պահուստավորումը սովորաբար կատարվում է արտաքին «կոշտ կրիչի վրա», սակայն կարող է լինել նաև «ամպային» պահուստում: «Ամպային» պահուստավորման դեպքում անհրաժեշտ է համոզվել, որ նման ծառայություններ տրամադրող կազմակերպությունը ունի բավարար մակարդակի պաշտպանության համակարգ: Օրինակ, ISO/IEC 27017 սերտիֆիկատը կարող է վկայել, որ «ամպային» պահուստավորման ծառայություն մատուցողը ունի բավարար պաշտպանության մակարդակ:

Պարբերաբար, սակայն ոչ պակաս քան տարին մեկ անգամ, անհրաժեշտ է ստուգել պահուստավորված տեղեկությունների վերականգման արդյունավետությունը, որպեսզի չստացվի, որ անհրաժեշտության դեպքում ինչ-որ տեխնիկական պատճառներով այն հնարավոր չի վերականգնել:

8.2. Աշակման ընթացքում գտնվող տվյալներ (data in use)

Աշակման 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: Այդ ժամանակը կարող է լինել 15 - 30 րոպե:

Հեռահար աշխատանքը խոհրդապահական տվյալներ կամ տեղեկություններ պարունակող բազաների հետ որպես կանոն պետք է արգելվի: Առանձին ծայրահեղ անհրաժեշտ դեպքերում այն կարող է թույլատրվել համակարգի տնօրենի (system administrator) վերահսկողության ներքո՝ պահպանելով անվտանգության բոլոր կանոնները, այդ թվում կետից-կետ VPN միացում (point-to-poin VPN), բազմակի նույնականացում (օրինակ հեռախոսով կամ անվտանգ հաղորդագրության ծրագրով - secure messanging application) և որպես կանոն ստատիկ IP և հայտնի MAC հասցեից:

8.3. Հաղորդվող տվյալներ (data in motion)

Դյուրակիր կրիչների վրա պահպանվող խորհրդապահական տվյալները պետք է պարտադիր լինեն պաշտպանված գաղտնաբառով և գաղտնագրված: Այն դեպքում, երբ տվյալները պետք է հաղորդվեն էլեկտրոնային հաղորդակցության միջոցներով՝ էլեկտրոնային փոստով կամ ներբեռնվեն այլ գրասենյակում կամ կազմակերպությունում գտնվող սերվերից կամ համակարգչից, տվյալները պետք է ևս լինեն գաղտնագրված ու պաշտպանված հուսալի բանալիով: Հուսալի բանալիների երկարությունը տարբերվում է՝ ըստ դրանց ստանդարտների ու ալգորիթմների և ժամանակ առ ժամանակ վերանայվում է: SS և անվտանգության մասնագետները պետք է պարբերաբար ստուգեն օգտագործվող գաղտնագրման բանալիների հուսալի երկարությունը:

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:

9. Պատահարների դեպքում արձագանքը, վերականգնումը և շարունակականությունը

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, 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: Միևնույն ժամանակ տեղեկատվական պատահարը կարող է առհասարակ կապ չունենալ համակարգչային հարձակման հետ, այլ լինել ներքին արտահոսք կամ աշխատանքային անփութության արդյունք: Անվտանգության պատահար չհամարվող դեպքերը կոչվում են անվտանգության իրադարձություն:

Օրինակ, աշխատակիցը կարող է կանխամտածված փոխանցել որևէ մեկին այլ անձանց տվյալները կամ սխալմամբ ուղարկել խորհրդապահական տեղեկատվություն մեծ թվով անձանց: Դա համարվում է տեղեկատվական անվտանգության պատահար, որը պետք է ստանա արձագանք: Վնասակար ծրագրի ներթափանցման կանխումը էլեկտրոնային փոստի սերվերում տեղադրված պաշտպանիչ համակարգի կողմից տեղեկատվական պատահար չի համարվում, քանի որ պաշտպանիչ համակարգը ճիշտ է տեղադրվել և պատշաճ արձագանքել է: Պարագծային հրապատի ներթափանցումը, որը հաջողվել է կանխել սերվերում գտնվող պաշպանիչ համակարգի շնորհիվ համարվում է տեղեկատվական պատահար, քանի որ պարագծային հրապատը չի կանխել ներթափանցումը ու այն խափանվել է այլ հատվածում:

Բոլոր աշխատակիցները պետք է իրազեկված լինեն և իմանան՝ ինչպես գործել տեղեկատվական պատահարները դեպքում: Առաջին և ամենակարևոր գործողությունը անվտանգության կամ SS մասնագետին պատահարի մասին հայտնելն է: Աշխատակիցները կարող են չտարբերակել պատահարները իրադարձությունից, և դրա անհրաժեշտությունը չկա: Ցանկացած դեպքում պետք է տեղեկացնեն անվտանգության կամ SS մասնագետին իրենց հայտնի դարձած անվտանգության հետ կապված դեպքերի մասին, իսկ պատահար է դա, թե իրադարձություն, կորոշի մասնագետը:

Տեղեկանալով պատահարի մասին անվտանգության (SS) մասնագետը առաջին հերթին պետք է պարզի շարունակվում է արդյոք պատահարը, այն փորձ է թե ավարտված հարձակում, կա տվյալների արտահոսք թե ոչ: Եթե հարձակումը շարունակվում է, կամ արտահոսքը կարելի է կանխել, վերացնել կամ նվազեցնել, կամ հանգամանքները պահանջում են արագ արձագանք, ապա 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 կամ արտահոսք կամ տեղի է ունենում նպատակաուղղված շարունակական վտանգ/հարձակում (advanced persistant threat), անհրաժեշտ է նաև հայտնել այդ մասին համապատասխան իրավապահ մարմինների՝ Ազգային անվտանգության ծառայություն կամ ոստիկանության համակարգչային հանցագործությունների ստորաբաժանում:

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 ունցել, երբ և ինչպես քաղաքացիները կարող են պարզել վտանգված են իրենց տվյալները, թե ոչ և ինչ է անհրաժեշտ ձեռնարկել: Օրինակ, եթե պատահարի հերևանքով տեղի է ունեցել էլեկտրոնային հասցեների ու հեռախոսահամարների արտահոսք, ապա ցանկալի է պարզաբանել, որ այն կարող է վտանգել էլ փոստի երկակի նույնականացման եղանակը ու առաջարկել փոփոխել այն այլ եղանակով:

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: Ընդ որում, պետք է նշված լինեն և 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: Այն դեպքում, երբ բացերը լրացնել հնարավոր չէ՝ օրինակ, ֆինանսական կամ տեխնիկական

ռեսուրսների բացակայության պատճառով, մատյանում պետք է գրանցվեն և պատճառները, և այն բացերը, որոնք հնարավոր չի եղել լրացնել: Նման դեպքերում պետք է մշակել և իրագործել տեղեկատվական պատահարների հետևանքները կանխելու կամ վնասը նվազեցնելու միջոցառումների ցանկ:

10. Ծրագրակազմի անվտանգություն

10.1. Հեղինակային իրավունքը և լիցենզիաները

Ծրագրային անվտանգության հետ կապված միջոցները (software security controls) կարելի է բաժանել մի քանի ենթախնդրիի: Նախ անհրաժեշտ է նշել, որ ցանկացած համակարգում ոչ լիցենզավորված՝ այսինքն ապօրինի ձեռք բերված ծրագրերի ու համակարգերի օգտագործումն ինքնըստինքյան պարունակում է թե՛ իրավական, թե՛ կազմակերպչական, թե՛ տեխնիկական վտանգ: Այն կարող է ցանկացած պահի վերածվել հեղինակային իրավունքի: Համակարգի կամ ծրագրի աշխատանքի չնախատեսված կամ առնվազն անսպասելի դադարեցումը կարող է վտանգել մշակվող տվյալները, բազաները և այլ ծրագրերը:

Եթե կազմակերպությունում կա չլիցենզավորված ծրագրային ապահովում, անհրաժեշտ է մշակել դրա փոխարինման պլանը: Ոչ լիցենզավորված ծրագրերը կարող են փոխարինվել արդիական վճարովի ծրագրերով կամ ոչ արդիական ծրագրերով ու համակերգերով, որոնք սովորաբար ունեն ավել ցածր գին և, ի վերջո, կարող են փոխարինվել բաց կոդով անվճար ծրագրերով (ԲԿԾ): ԲԿԾ-րի կիրառումը կարող է պահանջել աշխատակազմի լրացուցիչ ուսուցում, որը սակայն ի վերջո կարող է զգալիորեն տնտեսել կազմակերպության ՏՏ ծախսերը, որոնք կարող են օգտագործել համակարգչային բազան արդիականացնելու կամ անվտանգության միջոցների ուժեղացնելու վրա:

Որպես կանոն, աշխատակիցները չպետք է իրավունք ունենան ինքնուրույն տեղադրել որևէ ծրագիր, մանավանդ ներբեռնելով այն հեմացանցից: Այդ դեպքերում, երբ նման անհրաժեշտություն կառաջանա այս կամ այն աշխատակցի աշխատանքը ավելի արդյունավետ կազմակերպելու համար, լրացուցիչ ծրագիր կարող է տեղադրվել կամ ներբեռնվել համացանցին ՏՏ կամ ՏՏ անվտանգության մասնագետի թույլտվությամբ:

Նախքան լրացուցիչ, ոչ ստանդարտ ծրագիր տեղադրելը կամ ներբեռնելը ՏՏ մասնագետը պարտավոր է ուսումնասիրել այդ ծրագիրը, ծանոթանալ ծրագիրը ստեղծած ընկերության վարկանիշին և այդ ծրագրի օգտագործման մասին ՏՏ հանրության արձագանքերին: Առավել զգուշություն է պետք դրսևորել, եթե նման ծրագիրն օգտագործվում է խորհրդապահական տվյալների մշակման համար: Ծրագիրը տեղադրելուց հետո սկզբնական փուլում պետք է ուշադիր հետևել ծրագրի աշխատանքին և նկատելով ծրագրի կողմից մեծ քանակով տվյալների փոխանակում այլ համակարգիչների կամ ցանցերի հետ, դադարեցնել դրա աշխատանքը ու փորձել ուսումնասիրել՝ որքանով դա անվտանգ է տվյալների անվտանգության առումով:

Կազմակերպության կողմից կամ պատվերով ստեղծված ծրագրերը պետք է պարտադիր անցնեն փորձարկում (testing) մասնագիտացված բարձր որակավորում ունեցող փորձագետների կամ ընկերությունների կողմից: Մասնավոր ընկերություններին ծրագիր պատվիրելու դեպքում պետք է ուշադրություն դարձնել լիցենզիոն պայմաններին, որոնք պետք է թույլ տան հետագայում ծրագիրը շահագործել նույնիսկ եթե ծրագիրը ստեղծած

ընկերությունը հրաժարի ծրագրի սպասարկումից: Նախընտրելի են, իսկ կրիտիկական համակարգերի դեպքում պարտադիր, բաց կոդով ծրագրերը:

Ծրագրային անվտանգության լավագույն պրակտիկա է համարվում աշխատանքային կայանների (համակարգիչներ), սերվերների և ցանցային սարքավորումներում օգտագործվող ծրագրերի և տվյալների բազաների գույքագրումը ու գույքագման արդյունքում կազմված ցուցակի պարբերական թարմացումը: Ծրագրերի ցուցակում յուրաքանչյուր համակարգչի դիմաց նշվում է օգտագործվող համակարգը, ծրագերը, լիցենզիաների տեսակները (օրինակ պրոպրիետար, բաց կոդով վճարովի, բաց կոդով անվճար և այլ) և դրանց ժամկետը:

10.2. Ծրագրային ապահովման 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:

10.3. Հակավիրուսային ծրագրեր և այլ 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: Սակայն 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:

10.4. Համացանցային ծրագրեր և կայքեր

Համացանցային կայքերը (web page) և իրենց հետ կախված ծրագրերը այսօր դարձել են կազմակերպությունների հիմնական աշխատանքային հարթակներից մեկը: Հաշվի առնելով այն, որ ներկայումս վեբ կայքերը օգտագործվում են ոչ միայն տեղեկատվություն հրապարակելու, այլ նաև հաճախորդների, քաղաքացիների և գործընկերների հետ համագործակցելու, ծառայություններ մատուցելու և սպասարկելու գործիք: Համացանցային կայքերը ստատիկ տեղեկատվական «վաղանակներից» ակտիվ փոփոխվող հարթակներին վերածվելը առաջացրել է տեղեկատվական անվտանգության հետ կապված մի շարք հարցեր:

Առաջին սկզբունքը, որ պետք է կիրառվի համացանցային կայքերի ստեղծման և շահագործման ժամանակ, այն է, որ համացանցային կայքերի հանդեպ պետք է կիրառվեն

անվտանգության նույն կանոնները, որոնք կիրառվում են համակարգում տեղադրված և շահագործվող ծրագրերի: Ծրագրերի օրինականությունը (հեղինակային լիցենզիաների առկայությունը), մասնագիտացված ընկերությունների կողմից անցկացրած փորձաքննությունը (տեստավորումը), պարբերաբար արդիականացումը (թարմացումը) և անվտանգության կարկատների հրատապ տեղադրումը:

Կայքերի հետ միացումը պետք է իրականացվի միայն անվտանգ արձանագրությունների օգտագործմամբ: Դրանք են TLS/SSL (Transport Leyer Security, Secure Socket Layer) արձանագրությունները: Առհասարակ համացանցային կայնքը տեղադրվում է «ապառազմականացված» գոտիներում (demilitarized zone) և դրանց կապը խորհրդապահական տվյալների հետ անմիջական չէ: Սակայն, կարող են լինել այլ լուծումներ՝ ներառյալ «ամպային կրիչների» օգտագործումը:

11. Տեղեկատվական անվտանգության շարունակականությունը

Տեղեկատվական անվտանգության ապահովումը շարունակական և անընդհատ կատարելագործվող գործընթաց է: Տեղեկատվական տեխնոլոգիաները առավել արագ փոփոխվող պոլիմերներից են և դրանց զարգացումը էականորեն ազդում է նաև տեղեկատվական անվտանգության մակարդակին և համակարգերի պաշտպանվածություն մակարդակին: SS և SS անվտանգության մասնագետները պետք է պարբերաբար ծանոթանալ համակարգչային և ցանցային նոր վտանգների մասին և մատչելի ձևով իրազեկեն աշխատակիցներին հնարավոր վտանգերնի ու դրանցից խուսափելու եղանակների վերաբերյալ:

Մասնավորապես կարևոր է հետևել արագ տարածվող նոր վնասակար ծրագրերին, արձանագրությունների խոցելիությունների, այս կամ այն տեխնոլոգիաների (օրինակ Wi-Fi, Bluetooth) խոցելիություններին, էլեկտրոնային փոստի, տվյալների բազաների ու օպերացիոն համակարգերի պաշտպանիչ գործիքները խոցելիություներին, համացանցային պլատֆորմների ու փնտրող ծրագրերի (browser) անվտանգության բեցերին: