Հավելված N 1
ՀՀ կառավարության 2012 թ.
հունիսի 14-ի նիստի N 23
արձանագրային որոշման

Ծ Ր Ա Գ Ի Ր
ՀԱՄԱԿԱՐԳՉԱՅԻՆ ՎԻՐՈՒՍԱՅԻՆ ՎՏԱՆԳԻ ԴԵՄ ԱՐԴՅՈՒՆԱՎԵՏ ՊԱՅՔԱՐ ԻՐԱԿԱՆԱՑՆԵԼՈՒ ՄԻՋՈՑԱՌՈՒՄՆԵՐԻ

I. ՆԱԽԱԲԱՆ

Առաջին համակարգչային վիրուսները հայտնվել են ավելի քան 20 տարի առաջ: Այդ ժամանակից ի վեր, սպառնալիքների բնույթը արմատապես փոխվել է՝ արտացոլելով փոփոխությունները տեխնոլոգիաներում, կյանքի բոլոր նոր ոլորտներում համակարգիչների ներդրումը և օգտվողների թվի անդադար աճը: Մարդկային գործունեության ցանկացած ոլորտում յուրաքանչյուր նոր սերունդ հերթափոխությունը ընդունում է իր նախորդից, որը հիմնվելով նրա նվաճումների վրա՝ կրկին կիրառում է այնպիսի տեխնիկա, որն ապացուցել է իր հաջողվածությունը, և միևնույն ժամանակ ձգտում է ստեղծել նոր ուղիներ: Սա վերաբերում է նաև վնասակիր ծրագրային կոդի հեղինակներին: Վիրուսային ծրագրերի հեղինակների մի քանի սերունդներ ամբողջությամբ փոխել են տեղեկատվական սպառնալիքների իրավիճակը:

Մի քանի տարի առաջ վիրուսների մեծամասնությունը սահմանափակվում էր համակարգչային սկավառակների և ծրագրերի աղտոտմամբ: Հիմնականում վնասը սահմանափակվում էր տվյալների կորստով, քանի որ վիրուսները մաքրում կամ (երբեմն) փչացնում էին սկավառակի վրայի տվյալները:

Այժմ ամեն ինչ այլ է: Այսօր կիբեռհանցագործությունը լայնածավալ խնդիր է: Վնասակիր ծրագրերը գրվում են անօրինական ճանապարհով այլ համակարգիչների օգտագործմամբ տեղեկատվություն ստանալու նպատակով:

Արդի հասարակությունը դժվար է պատկերացնել առանց հանցագործության, որն ազդում է կյանքի գրեթե բոլոր ոլորտների վրա: Այդ պատճառով էլ զարմանալի չէ, որ համակարգչային տեխնոլոգիաների կիրառումը կամ օգտագործումը զարգանում է չարաշահումների հետ համընթաց: Ավելին, կյանքի բոլոր նոր ոլորտներում համակարգիչների ներթափանցումը, հանցագործներին ավելի շատ հնարավորություններ է ընձեռում իրենց նպատակները իրականացնել նորագույն տեխնոլոգիաների միջոցով:

Այժմ կյանքի բոլոր ոլորտներում տեղեկատվական տեխնոլոգիաների զարգացման և համատարած ներդրման հետ կապված արդիական խնդիր է համարվում հուսալի տեղեկատվական համակարգերի կազմակերպումը և ապահովումը, որոնք կլինեն կազմակերպությունների աշխատանքների ապակայունացման ազդեցության կամ տեղեկատվության գողություն-

ների դեմ դիմացկունության, ինչպես նաև մշակվող և պահպանվող տվյալների արժանահավատության պահպանման հիմնական միջոցը:

II. ԾՐԱԳՐԻ ՄՇԱԿՄԱՆ ՀԻՄՔԵՐԸ

Ծրագրի մշակման համար հիմք են հանդիսացել `

1. 2009 թ. հունիսի 26-ի ՀՀ Նախագահի <<Հայաստանի Հանրապետության տեղեկատվական անվտանգության հայեցակարգը հաստատելու մասին>> թիվ ՆԿ-97-Ն կարգադրությունը,
2. <<Կիբերհանցագործությունների մասին>> կոնվենցիան,
3. ՀՀ-ում ներկայումս իրականացվող կիբեռանվտանգության գործընթացները,
4. 2010 թվականին փետրվարի 25-ին ՀՀ Կառավարության <<ՀՀ էլեկտրոնային հասարակության ձևավորման հայեցակարգը (2010–2012թթ.)>> N 7 արձանագրային որոշումը,
5. 2012 թվականի մարտին Ազգային անվտանգության խորհրդի կողմից հավանության արժանացած <<ՀՀ ահաբեկչության դեմ պայքարի ազգային ռազմավարությունը>>:

III. ՀԱԿԱՎԻՐՈՒՍԱՅԻՆ ՊԱՇՏՊԱՆՈՒԹՅԱՆ ՀԻՄՆԱԿԱՆ ԽՆԴԻՐՆԵՐԸ

Հակավիրուսային պաշտպանության հիմնական խնդիրները՝

1. Հուսալի տեղեկատվական համակարգերի ստեղծումը,
2. Հակավիրուսային միջոցների և նրանց թարմացման գործընթացը,
3. Հակավիրուսային միջոցների կիրառմամբ պրոֆիլակտիկ աշխատանքների անցկացումը,
4. Վիրուսներից կամ այլ վնասակար ծրագրերից տեղեկատվության անխափան և կայուն պաշտպանությունը,
5. Հակավիրուսային միջոցների կիրառմամբ էլեկտրոնային փոխանակման անվտանգության ապահովումը,
6. Հակավիրուսային հարցերով զբաղվող կազմակերպությունների հետ համագործակցութան կազմակերպումը և իրականացումը:

IV. ԾՐԱԳՐԻ ՆՊԱՏԱԿՆԵՐԸ

Ծրագրի նպատակներն են՝

1. Ստեղծել հուսալի տեղեկատվական համակարգեր,
2. Իրականացնել համակարգչային վիրուսների դեմ պայքարի միջոցառումների ծրագիր,
3. Իրականացնել վիրուսային համաճարակների ժամանակին հայտնաբերման և կանխարգելման միջոցառումներ:

V. ՀԱՄԱԿԱՐԳՉԱՅԻՆ ՎԻՐՈՒՍՆԵՐԻ ԴԵՄ ՈՒՂՂՎԱԾ ԱՐԴՅՈՒՆԱՎԵՏ ՊԱՅՔԱՐԻ ՄԻՋՈՑԱՌՈՒՄՆԵՐԸ

Համակարգչային վիրուսների դեմ պայքարը արդյունավետ իրականացնելու նպատակով անհրաժեշտ է իրականացնել հետևյալ միջոցառումները.

1. Համակարգչային տնտեսության և օպերացիոն համակարգերի առկայության ապահովում:

Ժամանակակից անվտանգության ստանդարտները ներկայացնում են համակարգչային ռեսուրսների բարձր պահանջներ (ՕՀՍ չափը, կենտրոնական պրոցեսորի հաճախականությունը) և ելնելով համակարգչային տնտեսության առկա վիճակից պետք է մշակել հուսալի տեղեկատվական համակարգի ապահովման միջոցառումներ:

Անհրաժեշտ է մշակել օպերացիոն համակարգի (թարմացումների ապահովմամբ) այնպիսի արդիական տարբերակ, որը կունենա գործող սարքավորումների վրա բավարար կատարողականություն և կլուծի առաջադրված խնդիրները:

2. Սերվերային տնտեսության առկայության ապահովում:

Անվտանգության ժամանակակից ստանդարտները սերվերային ռեսուրսներին ներկայացնում են բարձր պահանջներ (ՕՀՍ չափը, կենտրոնական պրոցեսորի հաճախականությունը) և ելնելով սերվերային տնտեսության արկա վիճակից պետք է մշակել հուսալի տեղեկատվական համակարգի ապահովման միջոցառումներ, այսինքն ցանցային սերվերների նվազագույն պահանջվող քանակ, ներխուժման դեմ պաշտպանություն ներխուժման փորձի և չարտոնված ցանցային ակտիվության մասին ահազանգման համակարգ:

3. Այլ ակտիվ ցանցային սարքավորումների առկայության ապահովում (երթուղավորիչներ, կառավարվող բաժանարար, ցանցային տպիչ, ցանցային կուտակիչ):

Կազմակերպության հաշվողական ցանցի ամբողջական սխեմայի ստեղծման ժամանակ պետք է վերլուծվեն և հաշվի առնվեն ցանցային սարքավորումները:

4. Ֆիզիկական ցանցի սխեմա:

Կազմակերպության ֆիզիկական ցանցի արդիական սխեմայի առկայությունը (որտեղ և ինչպես են անցկացված մալուխները, որտեղ են տեղադրված ակտիվ կամ պասիվ ցանցային սարքերերը) հնարավորություն է տալիս որոշել տեղեկատվական համակարգի հնարավոր վարակաբեր ուղիները և արտադրողականության, ինչպես նաև կայունության հնարավոր թույլ կողմերը:

5. Տրամաբանական ցանցի սխեմա:

Ելնելով կազմակերպության գործառույթների իրականացման պահանջներից, անհրաժեշտ է սահմանել համապատասխան գործառույթներ և միջոցներ (սերվերներ, երթուղավորիչներ,

ցանցային պահուստներ և այլն)՝ գոյություն ունեցող տեխնոլոգիաների միջոցով Ինտերնետ ցանցի միացման համար:

Ելնելով կազմակերպության գործունեությունից և օգտագործվող տվյալների արդիականությունից, սահմանել Ինտերնետ հասանելիության կանոններ և պահանջվող արտադրողականություն, ինչպես նաև հաճախորդների և սերվերի օպերացիոն համակարգերի արդիականության ապահովման գոյություն ունեցող տեխնոլոգիաներ:

Որոշել, թե որքան արդյունավետ են թարմացվում, ինչպես օպերացիոն համակարգերը, այնպես էլ ցանցային սարքերի ծրագրային ապահովումը՝ երթուղավորիչները, կառավարվող սվիչերը, տպիչների սերվերները և ցանցային պահուստները:

6. Հուսալի տեղեկատվական համակարգերի ստեղծման համար առաջնահերթությունների սահմանումը:

Ակնհայտ է, որ հուսալի տեղեկատվական համակարգերի անհապաղ իրականացում անհնար է, դրա համար անհրաժեշտ է կենտրոնանալ առավել կարևոր նշանակություն ունեցող ոլորտների վրա:

Այդպիսիք են՝

1) Օպերացիոն համակարգի ապահովումը տվյալ պահին արդիական անվտանգության թարմացման համակարգով,

2) Կազմակերպությունում իրականացնել թարմացման կենտրոնացված հակավիրուսային ծրագրային ապահովման տեղակայում:

7. Կազմակերպության ներքին էլեկտրոնային փաստաթղթաշրջանառության չափորոշիչների սահմանումը:

Կազմակերպության ներքին կորպորատիվ սերվերների օպտիմալ օգտագործումը ֆայլերի փոխանցման և ֆայլերի պահպանման օգտահործման չափորոշիչների ներդրում էլեկտրոնային փոստի և փաստաթղթաշրջանառության համակարգի համար, որը զգալիորեն կնվազեցնի կազմակերպության տեղեկատվական համակարգի չարամիտ վարակման վտանգը:

ISO/IEC 15408 չափորոշիչներին համապատասխան կազմակերպության ցանցի նախագծման համար փորձագետների ներգրավում և խնդիրների կատարման ապահովում:

Հաշվի առնելով օգտագործվող տեխնոլոգիաների փոխադարձ կախումը և աճող բարդությունը՝ ավելի արդյունավետ նախագծման և անվտանգության լուծումների ներդրման համար ներգրավել համակարգային ինտեգրատորների և փորձագետների:

8. Ինտերնետ ցանցի հետ կապված համակարգի գույքագրումը և բնորոշումը:

Համակարգերի ցուցակի կազմում, որոնք ունեն դեպի Ինտերնետ մուտք և կարևոր տեղեկություններ են պարունակում (օրինակ՝ հաշվապահական հաշվառում), ռեսուրսների ցուցակի կազմում, որոնք մատչելի են նման համակարգիչներից: Դա հնարավորություն կտա գաղտնի տեղեկատվության արտահոսքի նվազեցում:

9. Ծրագրի իրականացման ժամանակահատվածի և միջոցառումների համար անհրաժեշտ ռեսուրսների սահմանումը:

Վերը նշված միջոցառումների իրականացումից հետո հնարավոր է կատարել անհրաժեշտ փոփոխությունների հաշվարկ, ինչպես նաև սահմանել իրականացման ժամկետներ: Սովորաբար հակավիրուսային և օպերացիոն համակարգերի թարմացման համակարգի ներդրման համար բավարար ժամկետ է հանդիսանում 1-3 շաբաթը:

10. Հուսալի տեղեկատվական համակարգերի ապահովման համար միջոցառումներ:

Կազմակերպության տեղեկատվական համակարգերի ստեղծումը և պահպանումը անընդհատ գործընթաց է, որը պահանջում է անընդհատ ուշադրություն աշխատակիցների կողմից, իսկ ղեկավարության կողմից՝ հսկողություն: Նախանշված նպատակին հասնելու համար, որպես երաշխավոր հիմնականում հանդիսանում է մարդկային գործոնը:

11. Սպասարկող անձնակազմի ուսուցումը և հավաստագրումը:

Ներկայումս տեղեկատվական անվտանգության ոլորտում որակյալ մասնագետների կարիք կա: Պահանջվում է անցկացնել, ինչպես հիմնական (ցանցի հիմունքներ, օպերացիոն համակարգեր) այնպես էլ խորացված (ցանցային անվտանգություն, արձագանքում պատահարներին) դասընթացներ:

Հաշվի առնելով այն հանգամանքը, որ CISCO ընկերության ակտիվ ցանցային սարքավորումները լայն տարածում ունեն, նպատակահարմար է իրականացնել տվյալ սարքավորմների տիրապետման ուսուցում և հավաստագրում: Ինչպես նաև անհրաժեշտ է ուշադրություն դարձնել Microsoft ընկերության արտադրանքնի հետ աշխատող և (LPI, Linux Professional Institute Certification) բաց տարբերակով աշխատող անձնակազմի ուսուցմանը: Կախված կիրառվող տեխնոլոգիայից, իրականացնել ուսուցում և դրան հաջորդող անձնակազմի հմտությունների գնահատման հավաստագրում:

12. Փաստաթղթերի հասանելիության իրականացման համար անհրաժեշտ ծրագրային և սարքավորումների ապահովում:

Տեղեկատվության չարտոնված փոփոխման կամ պատճենահանման պաշտպանությունը հանդիսանում է առաջնային խնդիրներից մեկը: Այդ խնդիրը իրականացնելու համար անհրաժեշտ է՝

1) Որոշել համակարգի փաստաթղթերի ցանկը, որոնք ենթակա են վերահսկման և պաշտպանության
2) Որոշել անձնակազմի համար հասանելիության մակարդակը
3) Ընտրել անվտանգության տեխնոլոգիան և մոնիթորինգը
4) Ներդնել անվտանգության համակարգ և նշանակել պատասխանատու անձ:

13. Օպերացիոն համակարգերի վարակման բացառումը (նվազագույնի հասցնելը) վնասակար և լրտեսական ծրագրերով:

Այժմ օպերացիոն համակարգերը հանդիսանում են գերբարդ կառույցներ բազմաթիվ մոդուլներով և կախվածությամբ: Ցանկացած համակարգ ունի խոցելիություն և դրանց վերացման համար թողարկվում են թարմացման համակարգեր: Ուստի հրամայական է ապահովել օպերացիոն համակարգերի և վերահսողության ընթացակարգերի տեխնոլոգիաների շարունակական արդիականացումը: Թարմացման համակարգերի անջատման դեպքում օգտագործվող ցանկացած հակավիրուսային արտադրանք պաշտպանություն չի ապահովում: Հակավիրուսային ծրագրային ապահովոմը անհրաժեշտ է իրականացնել Հուսալի Տեղեկատվական Համակարգերի և չարակամ ծրագրերի պաշտպանությունից (Չարակամ ծրագիր (անգլ. malware, malicious software - <<կանխամտածված ծրագրային ապահովում>>): Ցանկացած ծրագրային ապահովում, որը նախատեսված է ձեռք բերել չարտոնված մուտք դեպի էլեկտրոնային հաշվողական մեքենայի (ԷՀՄ) անմիջապես հաշվողական ռեսուրսներ և տեղեկատվական համակարգ, նպատակ է հետապնդում տնօրինողի կողմից համակարգչային ռեսուրսների չարտոնված օգտագործման կամ տեղեկատվություն տնօրինողին վնաս հասցնելու (վնաս պատճառել) և/կամ ԷՀՄ-ի տնօրինողին, և/կամ ԷՀՄ-ի ցանցի տնօրինողին, պատճենահանման եղանակով, աղավաղման, վերացման կամ տեղեկատվության փոխարինման եղանակով:

14. Ակնկալվող արդյունքները:

Ստեղծել կայուն Հուսալի Տեղեկատվական Համակարգեր օգտվողների համար հարմարավետության առավելագույն մակարդկով և հերթական սպասարկման նվազագույն ժամանակի ծախսով: Դա թույլ կտա անձնակազմին կենտրոնանալ այն խնդիրների վրա, որոնք կնպաստեն տեղեկատվական համակարգերի հետագա զարգացմանը և ժամանակակից մարտահրավերներին համապատասխան նոր չափորոշիչների մշակմանը:

15. Վերահսկողություն:

Աշխատանքների կատարման վերահսկողությունը հնարավորություն է տալիս իրականացնել այն ժամանակին, ինչպես նաև չնչին են նախագծից շեղումները: Գոյություն ունեն տեղեկատվական անվտանգության միջազգային չափորոշիչներ, որտեղ ISO/IEC 15408-ը առավել արդիական է առաջադրված խնդրի լուծման համար:

16. Իրականացված միջոցառումների փորձաքննություն:

Հուսալի տեղեկատվական համակարգերի ապահովման համար կատարված բոլոր աշխատանքները պետք է փաստաթղթավորվի և անկախ փորձագետների կամ աուդիտորների կողմից պետք է պարբերաբար ստուգվի հաստատված ընթացակարգերի համապատասխանությունը, անկախ փորձագիտական խումբ կարող է հանդիսանալ Համակարգչային պատահարների արձագանքման խմբերը (CERT):

VI. ԾՐԱԳՐՈՎ ՆԱԽԱՏԵՍՎԱԾ ՄԻՋՈՑԱՌՈՒՄՆԵՐԻ ԻՐԱԿԱՆԱՑՄԱՆ ՊԱՏԱՍԽԱՆԱՏՈՒՆԵՐԸ

Սույն ծրագրով հաստատված միջոցառումների ժամանակացույցով նախատեսված միջոցառումները իրականացնում է ՀՀ տրասնպորտի և կապի նախարարությունը՝ հանրապետական գործադիր մարմինների կողմից տրամադրված տեղեկատվության հիման վրա՝ վերջիններիս համակարգչային վիրուսային վտանգից ապահովելու նպատակով:

VII. ԾՐԱԳՐԻ ՖԻՆԱՆՍԱԿԱՆ ԱՊԱՀՈՎՈՒՄԸ

Ծրագրով նախատեսված միջոցառումների իրագործման ֆինանսավորման աղբյուր են հանդիսանալու դոնոր կազմակերպությունների և մասնավոր հատվածի կողմից տրամադրված ֆինանսական միջոցները: