DIGIFENCE
TECHNOLOGY

27/4 Azatutyan Avenue
Yerevan 0014 Armenia
(374) 11 48 48 48
/digifence.tech
info@digifence.am
www.digifence.tech

Կիբեռանվտանգության հիմնական մակարդակ

▼ ՀՍԿՈՂՈՒԹՅԱՆ ՄԻՋՈՑ 01

Ապարատային սարքերի գույքագրում և վերահսկում

ՆՊԱՏԱԿԸ

Ակտիվորեն կառավարել (գույքագրել, հետևել և ուղղել) ցանցում գտնվող բոլոր ապարատային սարքերը, որպեսզի հասանելիությունը թույլատրվի միայն արտոնված սարքերին, իսկ չարտոնված սարքերի հասանելիությունը հայտնաբերվի և կանխվի:

ԿԱՐԵՎՈՐՈՒԹՅՈՒՆԸ

Աշխարհի ցանկացած կետում գտնվող հաքերները շարունակաբար սկանավորում են թիրախային կազմակերպությունների ցանցային հասցեները՝ հնարավոր անպաշտպան համակարգեր գտնելու նպատակով: Նրանք հատկապես հետաքրքրված են շարժական սարքերով, որոնք կարող են լինել ոչ համահունչ անվտանգության թարմացումներին կամ արդեն իսկ վարկաբեկված են: Հարձակումները կարող են ուղղված լինել նոր ապարատային սարքին, որը տեղադրված է ցանցում ընդամենը մեկ օր առաջ, բայց կարգավորված չէ և համապատասխան անվտանգության թարմացումները կիրառված չեն: Նույնիսկ համացանցից հասանելիություն չունեցող սարքերը կարող են հաքերների կողմից ենթարկվել հարձակման արդեն իսկ վարկաբեկված ներքին համակարգի միջոցով: Հավելյալ համակարգերը, որոնք կապված են կազմակերպության ցանցին (օրինակ՝ ժամանակավոր փորձարկման համար նախատեսված համակարգերը, հյուր ցանցերը) պետք է կառավարվեն և/կամ մեկուսացվեն՝ կազմակերպության անվտանգությունն ապահովելու և հաքերների մուտքը կանխելու համար:

Մեծ կազմակերպությունները պայքարում են արագ փոփոխվող միջավայրերի հետ, սակայն հաքերները արդեն իսկ ցուցադրել են համբերություն և կարողություն ակտիվները մեծ մաշտաբով «գույքագրելու և կառավարելու»՝ դրանց հնարավորությունները շահագործելու համար:

Համակարգչային սարքերի կառավարվող հսկողությունը նույնպես կարևոր դեր է խաղում համակարգի կրկնօրինակի պլանավորման ու իրականացման, պատահարների արձագանքման և վերականգնման հարցում:

▼ ՀՍԿՈՂՈՒԹՅԱՆ ՄԻՋՈՑ 02

Ծրագրային ակտիվների գույքագրում և վերահսկում

ՆՊԱՏԱԿԸ

Ակտիվորեն կառավարել (գույքագրել, հետևել և ուղղել) ցանցում գտնվող ամբողջ ծրագրային ապահովումը՝ միայն արտոնված ծրագրերի տեղադրումը և գործարկումը թույլատրելու, իսկ չարտոնված ծրագրերը հայտաբերելու և դրանց տեղադրումը կանխելու նպատակով:

ԿԱՐԵՎՈՐՈՒԹՅՈՒՆԸ

Հաքերները շարունակաբար սկանավորում են թիրախային կազմակերպությունները փնտրելով ծրագրերի խոցելի տարբերակներ, որոնք կարող են շահագործվել հեռակա կերպով: Որոշ հաքերներ տարածում են նաև վնասաբեր վեբ էջեր, էլեկտրոնային ու մեդիա ֆայլեր և այլ կոնտենտ՝ սեփական վեբ էջերի կամ վստահելի երրորդ կողմի կայքերի միջոցով: Նման բովանդակությանը խոցելի բրաուզերի կամ այլ ծրագրի միջոցով հասանելիություն ստանալու դեպքում, հաքերները վարկաբեկում են համակարգը տեղադրելով վնասաբեր ծրագրեր՝ ստանալով համակարգի հանդեպ երկարաժամկետ վերահսկողություն:

Որոշ հմուտ հաքերներ կարող են շահագործել նախկինում անհայտ խոցելիությունները, որոնց համար ծրագրային ապահովման մատակարարը անվտանգության թարմացումներ դեռ չի թողարկել: Առանց համապատասխան գիտելիքների կամ կազմակերպությունում տեղակայված ծրագրային ապահովման հսկողության անհնար է ապահովել ակտիվների պատշաճ անվտանգությունը:

Թույլ վերահսկվող համակարգչային սարքերը հավանական է լինեն կա՛մ գործող ծրագրեր, որոնք կիրառելի չեն բիզնես նպատակներով օգտագործման համար (առաջ բերելով պոտենցիալ անվտանգության խնդիրներ), կա՛մ վնասաբեր ծրագրեր՝ տեղակայված հաքերի կողմից համակարգ ներխուժումից հետո: Եթե նույնիսկ մեկ համակարգչային սարք է վարկաբեկված, հաքերները օգտագործում են այն, ինչպես նաև դրա հետ հաղորդակցվող այլ համակարգերը՝ զգայուն տեղեկատվություն ստանալու համար: Ավելին, վարկաբեկված համակարգչային սարքերը օգտագործվում են որպես մեկնարկի կետ համակարգչային ցանցերով տեղաշարժման համար: Այսպիսով, հաքերները կարող են արագորեն անցում կատարել մեկ վարկաբերված համակարգից դեպի այլ համակարգեր: Կազմակերպությունները, որոնք չեն կատարում ամբողջական ծրագրային ապահովման գույքագրում, չեն կարող գտնել խոցելի կամ վնասաբեր ծրագրերով համակարգեր՝ խնդիրները նվազեցնելու կամ հաքերներին զերծ պահելու համար:

Ծրագրային ապահովման կառավարվող հսկողությունը նույնպես կարևոր դեր է խաղում համակարգի կրկնօրինակի պլանավորման ու իրականացման, պատահարների արձագանքման և վերականգնման հարցում:

▼ ՀՍԿՈՂՈՒԹՅԱՆ ՄԻՋՈՑ 03
Շարունակական խոցելիության կառավարում

ՆՊԱՏԱԿԸ

Շարունակաբար ձեռք բերել, գնահատել և հաշվի առնել նոր տեղեկատվությունը՝ խոցելիությունների բացահայտման, վերականգնման և հաքերների հնարավորությունների նվազեցման նպատակով:

ԿԱՐԵՎՈՐՈՒԹՅՈՒՆԸ

Կիբեռ անվտանգության մասնագետները պետք է աշխատեն նոր տեղեկատվության անընդմեջ հոսքի հետ, ինչպիսիք են՝ ծրագրային թարմացումները և ուղղումները, անվտանգության վերաբերյալ խորհրդատվությունը, սպառնալիքի վերաբերյալ տեղեկատվությունը: Խոցելիությունների կառավարումը շարունակական գործընթաց է, որը պահանջում է բավականին ժամանակ, ուշադրություն և միջոցներ: Հաքերներին հասանելի է նույն տեղեկատվությունը, ինչը հնարավորություն է տալիս օգտվել նոր գիտելիքի և շտկման միջև եղած բացերից: Օրինակ, երբ հետազոտողները տեղեկացնում են նոր խոցելիությունների մասին, բոլոր կողմերը, ներառյալ՝ հաքերներ, մատակարարներ և կիբեռ անվտանգության մասնագետներ սկսում են համապատասխանաբար հարձակվողական, անվտանգության թարմացումների թողարկման և պաշտպանական աշխատանքները:

Կազմակերպությունները, որոնք չեն սկսանավորում խոցելիությունները և շտկում հայտնաբերված խնդիրները, հավանաբար ունեն վարկաբեկված համակարգչային սարքեր: Կիբեռ անվտանգության մասնագետները բախվում են հիմանական խնդիրների հետ կազմակերպության շտկման շրջանակը ընդլայնելու, նախաձեռնած միջոցների իրագործման և առաջնահերթությունը դասակարգելու գործընթացներում՝ հաշվի առնելով կոնֆլիկտային առաջնահերթությունն ու երբեմն անորոշ կողմնակի ազդեցությունը:

▼ ՀՍԿՈՂՈՒԹՅԱՆ ՄԻՋՈՑ 04
Ադմինիստրատիվ արտոնությունների վերահսկվող կիրառություն

ՆՊԱՏԱԿԸ

Կառավարել գործընթացներն ու գործիքները նախատեսված հետևելու/վերահսկելու/կանխարգելելու/ուղղելու ադմինիստրատիվ արտոնությունների կիրառությունը և կարգավորումը՝ համակարգիչներում, ցանցերում և ծրագրերում:

ԿԱՐԵՎՈՐՈՒԹՅՈՒՆԸ

Ադմինիստրատիվ արտոնությունների չարաշահումը առաջնային մեթոդ է ներխուժելու թիրախային կազմակերպություն: Երկու ընդհանուր հարձակվողական տեխնիկաներն օգտագործում են անվերահսկվող ադմինիստրատիվ արտոնությունները: Առաջինում աշխատակայանը աշխատում է արտոնյալ օգտատերով, ով շփոթմամբ բացում է էլեկտրոնային նամակի վնասաբեր կցորդը՝ բեռնելով վտանգավոր կայքէջից ֆայլ կամ պարզապես այցելում է կայքէջի վտանգավոր կոնտենտ, որը կարող է ավտոմատ կերպով օգտագործել բրաուզերները: Ֆայլը պարունակում է գործարկվող կոդ, որը մեկնարկվում է կա՛մ ավտոմատ կերպով, կա՛մ օգտատիրոջ միջամտությամբ: Եթե օգտատերն ունի ադմինիստրատիվ արտոնություններ, հաքերը ամբողջությամբ վարկաբեկում է աշխատակայանը և կարող է տեղադրել վնասաբեր ծրագրեր ու հեռակառավարման ծրագրային ապահովում՝ ադմինիստրատիվ գաղտնաբառեր և այլ զգայուն տվյալներ գտնելու համար: Նմանատիպ հարձակումները կատարվում են էլեկտրանային փոստի միջոցով: Ադմինիստրատորը պատահաբար բացում է վնասաբեր կոնտենտ պարունակող էլեկտրոնային նամակը, այնուհետև վարկաբեկված համակարգը օգտագործվում է ցանցում գտնվող այլ համակարգերի վրա հարձակման առանցքային կետ ստանալու նպատակով:

Հաքերների կողմից կիրառվող երկրորդ ընդհանուր տեխնիկան արտոնությունների բարձրացումն է՝ ադմինիստրատիվ օգտատիրոջ գաղտաբառը վարկաբեկելու միջոցով թիրախային համակարգչային սարքավորմանը հասանելիություն ստանալու նպատակով: Եթե ադմինիստրատիվ արտոնություններն լայնորեն բաշխված են, հաքերից պահանջվում է ավելի քիչ ժամանակ համակարգերի վրա ամբողջական վերահսկաղություն ստանալու համար, քանի որ կան բազմաթիվ հաշիվներ, որոնք կարող են հաքերի համար հանդես գալ որպես միջոցներ դրանց ձեռքբերման հարցում:

▼ ՀՍԿՈՂՈՒԹՅԱՆ ՄԻՋՈՑ 05
Շարժական սարքերի, դյուրակիր համակարգիչների, սերվերների և աշխատակայանների ապարատային և ծրագրային անվտանգ

ՆՊԱՏԱԿԸ

Ստեղծել, կիրառել և ակտիվորեն կառավարել (հետևել, ներկայացնել, ուղղել) շարժական սարքերի, դյուրակիր համակարգիչնեիրի, սերվերների և աշխատակայանների անվտանգ կարգավորումը՝ օգտագործելով կարգավորման և փոփոխության կառավարման գործընթացները՝ հաքերների կողմից կանխելու խոցելի ծառայությունների և կարգավորումների շահագործումը:

ԿԱՐԵՎՈՐՈՒԹՅՈՒՆԸ

Արտադրողների և մատակարարների կողմից գործառնական համակարգերի և ծրագրերի համար նախատեսված նախնական կարգավորումները սովորաբար ուղղված են դեպի ոչ թե անվտանգություն, այլ հեշտ տեղակայում և օգտագործում: Հիմնական հսկողության միջոցները, բաց ծառայությունները և պորտերը, օգտատերերի նախնական հաշիները կամ գաղտնաբառերը, խոցելի պրոտոկոլները, նախնական տեղադրված չօգտագործվող ծառայությունները կարող են շահագործվել իրենց նախնական վիճակում: Անվտանգ կարգավորումներ մշակելը բարդ խնդիր է, որը պահանջում է բազմաթիվ տարբերակների վերլուծություն ճիշտ ընտրություն կատարելու համար: Անգամ անվտանգ կարգավորումը պետք է շարունակաբար կառավարվի՝ ծրագրային ապահովման թարմացման կամ ուղղման, նոր անվտանգության խոցելիության ի հայտ գալու կամ նոր գործառնական պահանջների սպասարկման անվտանգությունը պահպանելու համար: Հակառակ դեպքում հաքերները կգտնեն հնարավորություններ շահագործելու ցանցային ծառայությունները և ծրագրային ապահովումը:

▼ ՀՍԿՈՂՈՒԹՅԱՆ ՄԻՋՈՑ 06

Տեղեկամատյանների սպասարկում, մշտադիտարկում և վերլուծություն

ՆՊԱՏԱԿԸ

Հավաքագրել, կառավարել, վերլուծել իրադարձությունների աուդի մատյանները, որոնք կարող են օգնել հայտնաբերելու, հասկանալու կամ հարձակումից վերականգնվելու հարցում:.

ԿԱՐԵՎՈՐՈՒԹՅՈՒՆԸ

Անվտանգության տեղեկամատյանների և վերլուծությունների թերությունները թույլ են տալիս հաքերներին թաքցնելու իրենց վայրը, վնասաբեր ծրագրային ապահովումը և գործողությունները: Եթե նույնիսկ հայտնի է համակարգերի վարկաբեկման փաստը, առանց պաշտպանված և ամբողջական տեղեկամատյանների գրառումների հարձակման մանարամասները և հաքերների հետագա գործողությունները անտեսանելի են: Առանց աուդիտի տեղեկամատյանների, հարձակումը կարող է աննկատ լինել անորոշ ժամանակով և հասցված վնասները կարող են լինել անդառնալի:

Երբեմն տեղեկամատյանների գրառումները հարձակման միակ ապացույցն են հանդիսանում: Բազմաթիվ կազմակերպություններ պահպանում են աուդիտի գրառումները համապատասխանության ստուգման նկատառումներով: Հաքերները օգտագործում են այդպիսի կազմակերպությունների աուդիտի տեղեկամատյանները հազվադեպ դիտելու հանգամանքը և հետևաբար համակարգերի վարկաբեկված լինելու չիմացությունը: Տեղեկամատյանների վերլուծության բացակայության կամ թերի լինելու պատճառով հաքերները երբեմն ամիսներով կամ տարիներով իրենց հսկողության տակ են պահում վարկաբեկված համակարգչային սարքերը՝ առանց թիրախային կազմակերպության տեղյակ լինելու, նույնիսկ եթե հարձակման ակնհայտությունը գրանցվել է տեղեկամատյաններում: