DIGIFENCE
TECHNOLOGY

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

Կիբեռանվտանգության հիմնարար մակարդակ

▼ ՀՍԿՈՂՈՒԹՅԱՆ ՄԻՋՈՑ 07

Էլեկտրոնային փոստի և վեր-բրաուզերի պաշտպանություն

ՆՊԱՏԱԿԸ

Նվազեցնել հաքերների հնարավորությունները շահագործելու մարդկային վարքագիծը՝ վեբ-բրաուզերների և էլեկտրոնային փոստի համակարգերի հետ փոխազդեցության միջոցով:

ԿԱՐԵՎՈՐՈՒԹՅՈՒՆԸ

Վեբ-բրաուզերները և էլեկտրոնային փոստը ընդհանուր կետեր են համարվում հարձակման և ներխուժման համար՝ իրենց տեխնիկական բարդության, ճկունության, ինչպես նաև այլ համակարգերի ու կայքէջերի հետ իրենց ուղղակի փոխազդեցության պատճառով: Կոնտենտը կարող է ստեղծված լինել օգտատերին գրավելու կամ դրդելու համար, ինչը մեծապես բարձրացնում է ռիսկայնությունը և թույլ տալիս վնասաբեր կոդի օգտագործում, արժեքավոր տվյալների կորուստ և այլ հարձակումներ: Վերոնշյալ ծրագրերի միջոցով օգտատերերը կարող են փոխազդել անվստահելի միջավայրերի հետ դրանք պոտենցիալ թիրախներ են հանդիսանում ծրագրային կոդի շահագործման և սոցիալական ինժինիրինգի համար:

▼ ՀՍԿՈՂՈՒԹՅԱՆ ՄԻՋՈՑ 08

Վնասաբեր ծրագրերից պաշտպանություն

ՆՊԱՏԱԿԸ

Վերահսկել վնասաբեր կոդի տեղադրումը, տարածումը և կիրառումը կազմակերպությունում արդյունավետ դարձնելով ավտոմատացման օգտագործումը՝ ապահովելու պաշտպանության, տվյալների հավաքագրման և ուղղիչ գործողությունների արագ կիրառումը:

ԿԱՐԵՎՈՐՈՒԹՅՈՒՆԸ

Վնասաբեր ծրագիրը համացանցի սպառնալիքների անբաժանելի և վտանգավոր մասն է, քանզի այն ստեղծված է հարձակվելու համակարգերին, սարքերին և տվյալներին: Այն արագ տեղաշարժվող ու արագ փոփոխվող է և ներխուժում է ցանկացած քանակի կետերի միջոցով ինչպիսիք են աշխատակայանները, էլեկտրոնային փոստի կցորդները, վեբ էջերը, ամպային ծառայությունները, օգտատերերի գործողությունները և արտաքին կրիչները: Ժամանակակից վնասաբեր ծրագիրը ստեղծված է պաշտպանությունից խուսափելու, հարձակում գործելու կամ դրանք ապաակտիվացնելու համար:

Վնասաբեր ծրագրերից պաշտպանությունը պետք է գործի այս դինամիկ միջավայրում՝ լայնածավալ ավտամատացման, արագ թարմացման և ինտեգրման գործընթացներում, ինչպիսին է, օրինակ՝ պատահարներին արձագանքը: Այն պետք է նաև տեղակայվի հարձակման հնարավոր բազում կետերում՝ բացահայտելու, կանգնեցնելու տարածումը կամ կառավարելու վնասաբեր ծրագրի կիրառումը: Կազմակերպության անվտանգության փաթեթը կատարում է ադմինիստրատիվ գործառույթներ՝ ճշտելու թե արդյո՞ք բոլոր պաշտպանության միջոցներն են ակտիվ և ընթացիկ յուրաքանչյուր կառավարվող համակարգում:

▼ ՀՍԿՈՂՈՒԹՅԱՆ ՄԻՋՈՑ 09

Ցանցային պորտերի, պրոտոկոլների ու ծառայությունների սահմանափակում և հսկողություն

ՆՊԱՏԱԿԸ

Կառավարել (հետևել, վերահսկել, ուղղել) պորտերի, պրոտոկոլների և ցանցային սարքերի ծառայությունները կիրառությունը՝ հաքերների հարձակման համար հասանելի խոցելիությունների պատուհանը նվազեցնելու նպատակով:

ԿԱՐԵՎՈՐՈՒԹՅՈՒՆԸ

Հաքերները փնտրում են հեռակա հասանելի ցանցային ծառայություններ, որոնք խոցելի են շահագործման համար: Ընդհանուր օրինակները ներառում են թույլ կարգավորված վեբ սերվերներ, փոստային սերվերներ, ֆայլ և պրինտ ծառայություններ, նախնական տեղադրումով DNS սերվերներ, երբեմն առանց համապատասխան բիզնես կարիքի: Տարբեր ծրագրային փաթեթներ ավտոմատ կերպով տեղադրում են ծառայություններ և ակտիվացնում դրանք՝ որպես հիմնական ծրագրային փաթեթի տեղադրման մաս՝ առանց օգտատիրոջը կամ ադմինիստրատորին տեղեկացնելու: Հաքերները սկանավորում են այդպիսի ծառայությունները և փորձում են շահագործել դրանք՝ վարկաբեկելով օգտատերերի նախնական ID-ները և գաղտնաբառերը կամ լայնորեն հասանելի շահագործման համար նախատեսված ծրագրային կոդը:

▼ ՀՍԿՈՂՈՒԹՅԱՆ ՄԻՋՈՑ 10

Տվյալների վերականգնման հնարավորություններ

ՆՊԱՏԱԿԸ

Կառավարել կրիտիկական տեղեկատվության պահուստավորման համար օգտագործվող գործընթացները և գործիքները՝ համապատասխան մեթոդոլոգիայով ժամանակին դրա վերականգնման նպատակով:

ԿԱՐԵՎՈՐՈՒԹՅՈՒՆԸ

Հաքերների կողմից վարկաբեկված համակարգչային սարքերը հաճախակի ենթարկվում են կարգավորման և ծրագրային զգալի փոփոխությունների: Երբեմն հաքերները կատարում են նաև փոփոխություններ պահպանվող տվյալներում ՝ դրանով իսկ ազդելով կազմակերպության արդյունավետությանը: Երբ հաքերները բացահայտվում են, չափազանց դժվար է կազմակերպությունների համար առանց արժանահավատ տվյալների վերականգնման հնարավորության հեռացնել համակարգչային սարքի վրա հաքերի ներկայության ասպեկտները:

▼ ՀՍԿՈՂՈՒԹՅԱՆ ՄԻՋՈՑ 11

Ցանցային սարքերի անվտանգ կարգավորում, ինչպիսիք են, օրինակ՝ ֆայերվոլները, երթուղիչները և փոխանջատիչները

ՆՊԱՏԱԿԸ

Ստեղծել, իրականացնել և ակտիվորեն կառավարել (հետևել, ներկայացնել, ուղղել) տեղեկատվական ենթակառուցվածքի սարքերի անվտանգության կարգավորումը՝ կիրառելով անվտանգ կարգավորման և փոփոխությունների կառավարման մեթոդները՝ հաքերների կողմից խոցելի ծառայությունների և կարգավորումների շահագործումը կանխելու նպատակով:

ԿԱՐԵՎՈՐՈՒԹՅՈՒՆԸ

Արտադրողների և վերավաճառողների կողմից, տեղեկատվական ենթակառուցվածքի սարքերի համար նախնական կարգավորումները ուղղված են հեշտ օգտագործմանը, այլ ոչ թե անվտանգությանը: Բաց ծառայությունները և պորտերը, նախնական օգտագործման հաշիվերը (ներառյալ ծառայությունների հաշիվները) կամ գաղտնաբառերը, հին (խոցելի) պրոտոկոլների սպասարկումը, չօգտագործվող ծրագրի նախնական տեղադրումը հնարավոր են շահագործվել: Ցանցային սարքերի անվտանգ կարգավորումների կառավարումը մեկանգամյա իրադարձություն չէ, այն գործընթաց է, որը ներառում է կարգավորումների և թույլատրելի ցանցային հոսքերի շարունակական վերագնահատումը: Հաքերները կարող են օգտվել ցանցային սարքերի ժամանակի ընթացքում քիչ հուսալի դառնալուց, քանի որ օգտատերերը՝ ելնելով բիզնեսի յուրահատկություններից պահանջում են բացառություններ: Երբեմն բացառությունները տեղակայված և այնուհետև չկատարված են մնում, երբ դրանք արդեն բիզնես պահանջմունքների համար կիրառելի չեն: Որոշ դեպքերում, բացառության անվտանգության ռիսկը ոչ՛ վերլուծված է պատշաճ կերպով, ոչ՛ էլ համապատասխանեցրած բիզնես պահանջմունքներին և կարող է փոփոխվել ժամանակի ընթացքում: Հաքերները փնտրում են խոցելի նախնական կարգավորումներ, բացեր կամ անհամապատասխանություններ ֆայերվոլի կանոններում, երթուղիչներում և փոխանջատիչներում՝ օգտագործելով այս բացերը պաշտպանության միջոցները շրջանցելու համար: Նրանք շահագործում են այդ սարքերը ցանցերին հասանելիություն ստանալու համար, ցանցային հոսքը վերահասցեավորելու և տեղեկատվությունը հափշտակելու համար: Այսպիսի գործողությունների միջոցով հաքերը հասանելիություն է ձեռք բերում զգայուն տվյալների նկատմամբ, փոխում է կարևոր տեղեկատվությունը, կամ նույնիսկ վարկաբեկում է համակարգչային սարքերը՝ ցանցում այլ վստահված համակարգ ներկայացնելու նպատակով:

▼ ՀՍԿՈՂՈՒԹՅԱՆ ՄԻՋՈՑ 12
Սահմանային պաշտպանություն

ՆՊԱՏԱԿԸ

Բացահայտել/ կանխարգելել/ուղղել տեղեկատվական հոսքը վստահության տարբեր մակարդակների ցանցերից՝ ուշադրություն դարձնելով վնասող տվյալների վրա:

ԿԱՐԵՎՈՐՈՒԹՅՈՒՆԸ

Հաքերները կենտրոնանում են համակարգերի շահագործման վրա, որոնք հասանելի են համացանցից, ներառյալ ոչ միայն DMZ, այլ աշխատակայաններ և դյուրակիր համակարգիչներ, որոնք համացանցին ունեն հասանելիություն: Սպառնալիքները, ինչպես օրինակ՝ կազմակերպված կրիմինալ խմբերը, օգտագործում են ցանցային սարքերի և համացանցին հասանելություն ունեցող աշխատակայանների կարգավորումների և ցանցային ճարտարապետության թերությունները՝ ցանցային սարքերում կազմակերպության տեղեկատվական ենթակառուցվածք մուտք գործելու համար: Այնուհետև հաքերները օգտագործում են այդ սարքավորումները տեղեկատվական ենթակառուցվածք ավելի խորը ներփաթանցելու համար՝ տեղեկատվությունը հափշտակելու, փոփոխելու կամ մշտական մուտք ապահովելու՝ հետագա ներքին ցանցի վարկաբեկման նպատակով:

Բացի այդ, բազմաթիվ հարձակումներ տեղի են ունենում բիզնես գործընկերների ցանցերի միջև, քանի որ հաքերները անցնում են մի կազմակերպության ցանցից մյուսը՝ շահագործելով խոցելի համակարգերը: Ցանցային հոսքերը կառավարելու և հարձակման ու վարկաբեկված համակարգչային սարքերի ապացույցներ գտնելու նպատակով պաշտպանությունը պետք է լինի բազմաշերտ՝ հիմնվելով ֆայերվոլների, DMZ-ների և IPS-ների ու IDS-ների վրա: Նաև կրիտիկական է ֆիլտրել մտնող և դուրս եկող ցանցային հոսքը:

Հատկանշական է, որ ներքին և արտաքին ցանցերի միջև սահմանները՝ որպես կազմակերպությունների ներսում ու դրանց միջև փոխկապակցվածության բարձրացման արդյունք, ինչպես նաև անլար տեխնոլոգիաների տեղակայման արագ աճի պատճառ թուլանում են: Այս ամենը երբեմն թույլ է տալիս հաքերներին ստանալ ցանցին հասանելիություն՝ շրջանցելով սահմանային համակարգերը: Ինչևիցե, արդյունավետ անվտանգությունը հիմնված է անվտանգ կարգավորված սահմանային պաշտպանության վրա, ինչը բաժանում է ցանցերը սպառնալիքի տարբեր մակարդակների, օգտագործողների խմբերի, տվյալների և վերահսկման մակարդակների վրա: Սահմանային ցանցերի արդյունավետ բազմաշերտ պաշտպանությունը օգնում է նվազեցնելու հաջողված հարձակումների թիվը՝ թույլ տալով անվտանգության անձնակազմին կենտրոնանալու հաքերների վրա, ովքեր կարողացել են շրջանցել սահմանային սահմանափակումները:

▼ ՀՍԿՈՂՈՒԹՅԱՆ ՄԻՋՈՑ 13
Տվյալների պաշտպանություն

ՆՊԱՏԱԿԸ

Կառավարել տվյալների արտահոսքը կանխարգելող գործընթացներն ու գործիքները, մեղմել կորցված տվյալների ազդեցությունները և հավաստիանալ զգայուն տեղեկատվության գաղտնիության և ամբողջականության մասին:

ԿԱՐԵՎՈՐՈՒԹՅՈՒՆԸ

Տվյալները պահպանվում են բազմաթիվ տեղերում: Տվյալների լավագույն պաշտպանությունը ծածկագրման, ամբողջականության պաշտպանության և տվյալների կորստի կանխարգելման մեթոդներն են: Քանի որ կազմակերպությունները շարունակում են օգտվել ամպային ծառայությունների և հեռահար մուտքից, կարևոր է ձեռնարկել տվյալների արտահոսքը սահմանափակելու, ինչպես նաև դրանց վարկաբեկման հավանականությունը նվազեցնելու քայլեր:

Որոշ կազմակերպություններ ճիշտ չեն նույնականացնում և տարբերակում իրենց զգայուն ու կրիտիկական ակտիվները: Բազմաթիվ միջավայրերում, ներքին օգտատերերը ունեն հասանելիություն բոլոր կրիտիկական ակտիվներին կամ դրանց զգալի մասին: Զգայուն ակտիվները կարող են նաև ներառել համակարգեր, որոնք իրականացնում են ֆիզիկական համակարգերի կառավարում և հսկողություն (օրինակ՝ SCADA): Հերիք է միայն, որ հաքերները ներթափանցեն այսպիսի ցանց, նրանք կարող են հեշտությամբ գտնել և վերցնել կարևոր տեղեկությունը, առաջացնել ֆիզիկական վնաս կամ վնասել գործարքները նվազագույն դիմադրողականությամբ: Օրինակ, վերջին երկու տարիների ընթացքում, հաքերները հնարավորություն ունեին նույն մակարդակի հասանելիություն ձեռք բերել սերվերներում պահվող զգայուն տվյալների նկատմամբ: Բացի այդ կան օրինակներ կորպորատիվ ցանցի հասանելիության շահագործման ու վերահսկման, պատճառելով վնաս՝ ֆիզիկական ակտիվների միջոցով:

▼ ՀՍԿՈՂՈՒԹՅԱՆ ՄԻՋՈՑ 14
Հսկվող հասանելիություն հիմնված «Անհրաժեշտ է իմանալ» սկզբունքի վրա

ՆՊԱՏԱԿԸ

Կառավարել գործընթացներն ու գործիքները, որոնք օգտագործվում են հետևելու/վերահսկելու/ուղղելու անվտանգ հասանելիությունը կրիտիկական ակտիվներին (օրինակ՝ տեղեկատվությանը, ռեսուրսներին, համակարգերին) կախված անձանցից, համակարգչային սարքերից և ծրագրերից, որոնք, համաձայն ընդունված դասակարգմանը, ունեն հասանելիության անհրաժեշտություն այդ ակտիվներին:

ԿԱՐԵՎՈՐՈՒԹՅՈՒՆԸ

Տվյալների ծածկագրումը տալիս է վստահություն, որ նույնիսկ տվյալների վարկաբեկված լինելու պարագայում, դրանց նկատմամբ հասանելիություն ստանալը դառնում է անիմաստ: Ինչևիցե, հսկողության միջոցները պետք է լինեն ճիշտ կիրառված՝ տվյալների արտահոսքի սպառնալիքը նվազեցնելու համար: Բազմաթիվ հարձակումներ տեղի են ունենում ցանցի միջոցով, մինչդեռ այլոք ներառում են դյուրակիր համակարգիչների և զգայուն տեղեկատվություն պարունակող այլ համակարգչային սարքավորումների ֆիզիկական գողություն: Այսուհանդերձ, շատ դեպքերում զգայուն տվյալների արտահոսքը մնում է չբացահայտված, քանի որ չի մշտադիտարկվում: Տվյալների էլեկտրոնային և ֆիզիկականական շարժը պետք է ուսումնասիրվի՝ հաքերների ազդեցությունը նվազեցնելու նպատակով:

Վերահսկվող կամ զգայուն տվյալների հանդեպ հսկողության կորուստը կազմակերպությունների կողմից լուրջ սպառնալիք է բիզնես գործառնությունների, և պոտենցիալ սպառնալիք է ազգային անվտանգությանը: Մինչդեռ որոշ տվյալներ կորում են գողության կամ լրտեսության հետևանքով, այս խնդիրների զգալի մեծամասնությունը ծագում է թերի հասկացված պրակտիկաների, արդյունավետ քաղաքականության բացակայության և օգտատերերի սխալների պատճառով: Տվյալների կորուստը կարող են լինել օրինական գործողությունների արդյունք (ինպիսին է e-Discovery-ն իրավաբանական գործընթացների շրջանակներում), հատկապես, երբ գրառումների պահպանումն անարդյունավետ է կամ անկայուն:

Տվյալների ծածկագրումը, ինչպես ցանցային հոսքում, այնպես էլ պահպանման ժամանակ՝ նվազեցնում է դրանց վարկաբեկման հավանականությունը: Սա ճիշտ է գործընթացների և ծածկագրման գործընթացներին վերաբերող տեխնոլոգիաների պատշաճ մոտեցման պարագայում: Դրա օրինակ է ծածկագրման բանալիների կառավարումը բազում ալգորիթմներում: Ծածկագրման բանալիների գեներացումը, օգտագործումն ու ոչնչացումը պետք է հիմնված լինի ապացուցված գործընթացների վրա, ինչպես սահմանված է օրինակ՝ NIST SP 800-57 ստանդարտում:

Պետք է նաև ապահովել կազմակերպությունների շրջանակներում հայտնի և ստուգված գաղտնագրման ալգորիթմների կիրառումը, ինչպես նշված է NIST-ում: Ալգորիթմների և կազմակերպության կողմից օգտագործվող գաղտնագրման բանալիների երկարությունների տարեկան կտրվածքով վերագնահատումը նույնպես խորհուրդ է տրվում՝ հավաստիանալու, որ կազմակերպությունները չեն շեղվում իրենց տվյալների նկատմամբ կիրառվող պաշտպանությունից:Ամպային ծառայություններում տվյալներ պահպանող կազմակերպությունների համար կարևոր է հասկանալ դրանց վրա տարածվող հսկողության միջոցները և սահմանել ծածկագրման և գաղտնագրման բանալիների անվտանգության կիրառման լավագույն մեթոդները: Հնարավորության դեպքում բանալիները պետք է պահվեն անվտանգ միջավայրերում, ինչպեսին են օրինակ՝ Hardware Security Modules (HSM)-ները:

Տվյալների կորստի կանխումը (DLP) վերաբերում է մարդկանց, գործընթացների և օգտագործվող տվյալների (օրինակ՝ օգտագործողների գործողություններ), շարժման մեջ գտնվող տվյալների (օրինակ՝ ցանցային գործընթացներ), և պահպանվող տվյալների (օրինակ՝ պահուստավորված տվյալներ) պարունակության ստուգման և կենտրոնացված կառավարման շրջանակներում հսկող համակարգերի համապարփակ մոտեցմանը: Վերջին մի քանի տարիների ընթացքում ներդրումների նկատելի փոփոխություն է եղել սկսած ցանցի ապահովումից մինչև ցանցում անվտանգանգ համակարգերի ու տվյալների անվտանգության ապահովումը: DLP հսկողության միջոցները հիմնված են քաղաքականությունների վրա և ներառում են զգայուն տվյալների դասակարգում, կազմակերպության շրջանակներում բացահայտում, հսկողության միջոցների կիրառում, ինչպես նաև հաշվետվողականություն և աուդիտ՝ քաղաքականությանը համապատասխան:

▼ ՀՍԿՈՂՈՒԹՅԱՆ ՄԻՋՈՑ 15

Անլար հասանելիության վերահսկում

ՆՊԱՏԱԿԸ

Կառավարել գործընթացներն ու գործիքները հետևելու/ վերահսկելու/ կանխարգելելու/ ուղղելու անլար ցանցերի (WLANs), անլար հասանելիության կետերի և համակարգերի անվտանգ օգտագործումը:

ԿԱՐԵՎՈՐՈՒԹՅՈՒՆԸ

Տվյալների գողության գլխավոր դեպքերը ձեռնարկված են եղել անլար ցանցերի միջոցով արտաքինից հասանելիություն ստանալով կազմակերպությունների անլար կետերին՝ շրջանցելով սահմանային անվտանգության միջոցները: Անլար հաճախորդները կանոնավոր կերպով վարակվում են հեռահար շահագործման համար նախատեսված՝ օդանավակայաններում ու սրճարաններում տեղակայված հանրային անլար ցանցերի միջոցով: Վարկաբեկված համակարգերը այնուհետև օգտագործվում են դրանք թիրախային կազմակերպության ցանցին կրկին միանալու համար: Այլ կազմակերպությունները զեկուցում են իրենց ցանցերի վրա չլիազորված, քողարկված ներքին ցանց անսահմանափակ մուտք ունենալու նպատակով տեղակայված անլար հասանելիության կետերի բացահայտման մասին: Քանի որ նրանք չեն պահանջում ֆիզիկական կապեր, անլար սարքերը հաքերների համար երակարաժամկետ հասանելիություն են հանդիսանում դեպի թիրախային միջավայր:

▼ ՀՍԿՈՂՈՒԹՅԱՆ ՄԻՋՈՑ 16

Հաշվի մոնիթորինգ և վերահսկում

ՆՊԱՏԱԿԸ

Ակտիվորեն կառավարել համակարգի և ծրագրի հաշիվների ստեղծումը, կիրառությունը, հեռացումը՝ հաքերների կողմից դրանց օգտագործման հնարավորությունները նվազեցնելու նպատակով:

ԿԱՐԵՎՈՐՈՒԹՅՈՒՆԸ

Հաքերները հաճախ բացահայտում և շահագործում են օգտատերերի հաշիվները, կեղծելով դրանք՝ դժվարացնելով անվտանգության աշխատակիցների կողմից իրենց բացահայտման գործընթացը: Պայմանագրային աշխատակիցների և աշխատողների հաշիվները, որոնք ազատվել են աշխատանքից և հաշիվները, որոնք բացվել են Red Team-ի թեստավորման համար, բայց չեն հեռացվել, հաճախ են օգտագործվել վերոնշյալ կերպով: Ավելին, որոշ ներքին խախտողներ կամ նախկին աշխատակիցներ պայմանագրի դադարումից հետո դեռևս հասանելիություն են ունենում համակարգի հաշիվներին՝ պահպանելով չլիազորված հասանելիությունը կազմակերպության համակարգչային ցանց և զգայուն տվյալներ: