DIGIFENCE
TECHNOLOGY

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

Կիբեռանվտանգության կազմակերպչական մակարդակ

▼ ՀՍԿՈՂՈՒԹՅԱՆ ՄԻՋՈՑ 17

Անվտանգության վերաբերյալ իրազեկման և ուսուցման ծրագրի ստեղծում

ՆՊԱՏԱԿԸ

Կազմակերպության բոլոր ֆունկցիոնալ դերերի համար (դրանք կարևորելով բիզնեսի և դրա անվտանգության տեսանկյունից) նույնականացնել կազմակերպության պաշտպանության աջակցության համար անհրաժեշտ յուրահատուկ գիտելիքը, հմտությունները և կարողությունները, զարգացնել և իրականացնել գնահատման միասնական ծրագիր, բացահայտել բացերը և լրացնել դրանք քաղաքականության, գործառնական պլանավորման, ուսուցման և իրազեկման ծրագրերի միջոցով:

ԿԱՐԵՎՈՐՈՒԹՅՈՒՆԸ

Հատկանշական է, որ կիբեռպաշտպանությունը հիմնականում ընդունվում է որպես տեխնիկական մարտահրավեր, սակայն մարդկային վարքագիծը նույնպես կարևոր դեր է խաղում կազմակերպության հաջողության կամ խափանման գործում: Մարդիկ կարևոր գործառույթներ են կատարում համակարգի նախագծման, իրագործման, գործառնության, կիրառման և հսկողության յուրաքանչյուր փուլում: Օրինակներ են՝ ծրագրավորողները, ովքեր կյանքի ցիկլի սկզբնական շրջանում չեն հասկանա համակարգի խոցելիությունը արմատախիլ անելու հնարավորությունը; SS մասնագետները, ովքեր չեն կարողանա բացահայտել անվտանգության արտեֆակտները և տեղեկամատյանները, օգտատերերը, ովքեր ենթակա են սոցիալական ինժինիրինգի սխեմաներին, ինչպիսիք են ֆիշինգը, անվտանգության վերլուծաբանները, ովքեր պայքարում են նոր տեղեկատվության հետ համահունչ շարժվելու համար, ինչպես նաև ղեկավարությունը և համակարգի սեփականատերերը, ովքեր պայքարում են քանակապես գնահատելու այն դերը, որ կիբեռանվտանգությունը խաղում է ընդհանուր գործառնական/առաքելության ռիսկում և չունեն համապատասխան ներդրումային որոշումներ կայացնելու ողջամիտ տարբերակ:

Հաքերները շատ զգույշ են այս դեպքերի հանդեպ և օգտագործում են դրանք պլանավորելու իրենց գործողությունները, ինչպես օրինակ զգուշորեն ստեղծելու ֆիշինգային նամակները, որոնք անզգույշ օգտատերերի համար նման են սովորականի, օգտագործելով բացերը քաղաքականության և տեխնոլոգիայի միջև (օրինակ՝ քաղաքականությունները որոնք չեն պահանջում տեխնիկական կիրառում);,աշխատելով շտկման կամ տեղեկամատյանի գրառման միջև ընկած ժամանակահատվածում, օգտագործելով ոչ կրիտիկական համակարգերը ինչպես հետագա շարժման կետ կամ որպես ռոբոթներ:

Ոչ մի կիբեռ պաշտպանության մոտեցում չի կարող արդյունավետ կերպով լուծել կիբեռ ռիսկը՝ առանց դրա սկզբնապատճառի լուծման: Հակառակ դեպքում, ուժեղացնելով մարդկանց կիբեռանվտանգության իրազեկվածությունը, կարող ենք զգալիորեն բարձրացնել պատրաստակամությունը:

▼ ՀՍԿՈՂՈՒԹՅԱՆ ՄԻՋՈՑ 18
Ծրագրային ապահովման անվտանգություն

ՆՊԱՏԱԿԸ

Կառավարել բոլոր ներքին գրված ծրագրերի անվտանգության կյանքի ցիկլը՝ կանխելու, բացահայտելու և ուղղելու անվտանգության թույլ կողմերը:

ԿԱՐԵՎՈՐՈՒԹՅՈՒՆԸ

Հաքերները հաճախ օգտվում են վեբ և այլ ծրագրային ապահովման մեջ հայտնաբերված խոցելի կողմերից: Խոցելի կողմերը կարող են լինել տարբեր պատճառներով, ներառյալ կոդավորման սխալներ, տրամաբանական սխալներ, ոչ լիակատար պահանջների կատարում և անսովոր ու անսպասելի պայմանների թեստավորման ձախողում: Հատուկ սխալների օրինակներ են օգտատերերի մուտքագրման տվյալների ստուգման թերացումը, պոտենցիալ վնասաբեր բնույթի մուտքային սիմվոլների հաջորդականության ֆիլտրելու բացակայությունը, փոփոխականների սկզբնականացման և մաքրման ձախողումը, ինչպես նաև թույլ հիշողության կառավարումը՝ թույլատրելով հոսքերին ծրագրի մի հատվածում ազդելու ոչ կապված (և անվտանգության համար ավելի կարևոր) մասերի վրա:

Գոյություն ունի հանրային և մասնավոր տեղեկատվության մեծ պաշար այնպիսի խոցելիությունների մասին, որոնք թույլ են տալիս հաքերներին և անվտանգության մասնագետներին, ինչպես նաև գործիքների և տեխնիկաների հուսալի շուկային՝ թույլ տալ խոցելիությունների շահագործումը: Հաքերները կարող են օգտագործել հատուկ կոդեր ներառյալ բուֆերի գերլիցքավորումը, Structured Query Language (SQL) վնասաբեր հարձակումների, կայքերի խաչաձև սկրիպտինգի, կայքերի խաչաձև կեղծ հարցման և կոդի սեղման միջոցով խոցելի համակարգչային սարքերի վրա հսկողություն ստանալու նպատակով: Մեկ հարձակման մեջ, ավելի քանի 1 միլիոն վեբ սերվերներ շահագործվել և փոխվել են շահագործման գործիքների՝ SQL ներարկում օգտագործելով այցելուների համար: Այդ հարձակման ընթացքում, վստահելի վեբ կայքերը հաքերների կողմից պետական կառավարման և այլ կազմակերպություններից օգտագործվել են՝ հազարավոր բրաուզերներից այդ վեբ կայքերին հասանելիություն ունեցող հարյուրավորներին շահագործելու նպատակով: Բազմաթիվ վեբ և ոչ վեբ ծրագրային խոցելիություններ հայտնաբերվում են կանոնավոր կերպով:

▼ ՀՍԿՈՂՈՒԹՅԱՆ ՄԻՋՈՑ 19
Պատահարին արձագանք և կառավարում

ՆՊԱՏԱԿԸ

Պաշտպանել կազմակերպության տեղեկատվությունը, ինչպես նաև համբավը, պատահարին արձագանք կառուցելու և իրականացնելու միջոցով (օրինակ՝ պլաններ, սահմանված դերեր, ուսուցում, կոմունիկացիաներ, կառավարման վերահսկողություն), հարձակումը արագ բացահայտելու և այնուհետև արդյունավետ կերպով վնասը զսպելու, հաքերի ներկայությունը վերացնելու ու վերականգնելու ցանցային և համակարգային ամբողջականությունը:

ԿԱՐԵՎՈՐՈՒԹՅՈՒՆԸ

Կիբեռ պատահարները ներկայումս մեր կյանքի մաս են կազմում: Նույնիսկ մեծ, լավ ֆինանսավորված և տեխնիկապես բարդ կազմակերպությունը պայքարում է հարձակումների հաճախականության և բարդության դեմ: Կազմակերպության դեմ հաջողված կիբեռ հարձակման հարցը ոչ թե «եթե»-ն,այլ «ե՞րբ»-ն է:

Երբ պատահար է տեղի ունեցել, արդեն շատ ուշ է ճիշտ գործընթաց, հաշվետվության կազմում, տվյալների հավաքագրում, կառավարման պատասխանատվություն, օրինական պրոտոկոլներ, կոմունիկացիոն ստրատեգիա մշակելու համար, ինչը թույլ կտա կազմակերպությանը բարեհաջող կերպով հասկանալ, կառավարել և վերականգնվել : Պատահարին արձագանքի պլանի բացակայության պատճառով կազմակերպությունը չի կարող բացահայտել հարձակումը սկզբնական շրջանում, կամ եթե հարձակումն արդեն բացահայտված է, կազմակերպությունը չի կարող հետևել գործընթացներին՝ վնասը զսպելու, հաքերի ներկայությունը վերացնելու և անվտանգ կերպով վերականգնվելու համար: Այդպիսով հաքերը կարող է ունենալ ավելի խորը ազդեցություն, ավելի մեծ վնաս հասցնելով, ավելի շատ համակարգեր վարակելով, և ,հնարավոր է, ավելի շատ զգայուն տվյալներ արտաբերել, քան կարող էր հնարավոր լիներ արդյունավետ պատահարին արձագանքի պլան ունենալու դեպքում:

▼ ՀՍԿՈՂՈՒԹՅԱՆ ՄԻՋՈՑ 20

Ներթափանցման թեստեր և Red Team -ի վարժություններ

ՆՊԱՏԱԿԸ

Թեստավորել ամբողջությամբ կամակերպության պաշտպանությունը (տեխնոլոգիա, գործընթացներ և մարդիկ)՝ հաքերի նպատակներն ու քայլերը մոդելավորելու միջոցով:

ԿԱՐԵՎՈՐՈՒԹՅՈՒՆԸ

Հաքերները հաճախ շահագործում են լավ պաշտպանվող դիզայնների ու միտումների և իրականացման կամ պահպանման միջև եղած բացերը: Օրինակները ներառում են՝ խոցելիության հայտարարության, մատակարարի թարմացման հասանելիությունը և յուրաքանչյուր համակարգչային սարքի վրա ակտուալ տեղադրման միջև ընկած ժամանակը: Այլ օրինակներ են լավ մտածված քաղաքականությունները, որոնք չունեն տեխնիկական կիրառման մեխանիզմներ (հատկապես նրանք, որոնք սահմանափակում են մարդկանց ռիսկային գործողությունները), ցանց մուտք ու ելք լինող սարքավորումներին կարգավորումների կցման թերացումը և պաշտպանողական գործիքների կամ անվտանգությանը առնչություն ունեցող համակարգի գործառնությունների հասկացողության ձախողումը:

Հաջողված պաշտպանողական դիրքը պահանջում է արդյունավետ քաղաքականություններ և կառավարում, ուժեղ տեխնիկական պաշտպանություն և մարդկանց կողմից համապատասխան քայլեր: Բարդ միջավայրում որտեղ տեխնոլոգիան պարբերաբար զարգանում է և նոր հաքերներ են պարբերաբար հայտնվում, կազմակերպությունները պետք է ժամանակ առ ժամանակ թեստավորեն իրենց պաշտպանվածությունը՝ բացեր գտնելու և գնահատելու իրենց պատրաստակամությունը ներթափանցման թեստերի միջոցով:

Ներթափանցման թեստավորումը սկսվում է կազմակերպությունում խոցելիությունների իդենտիֆիկացման և գնահատման միջոցով: Այնուհանդերձ, թեստերը կազմված են և ձևակերպված յուրահատուկ ներկայացնելու՝ թե ինչպես հակառակորդը կարող է խափանել կազմակերպության անվտանգության նպատակները (օրինակ՝ հատուկ ինտելեկտուալ սեփականության պաշտպանություն) կամ հասնել հատուկ նպատակներին (օրինակ՝ C&C ստեղծում): Արդյունքները ավելի տեսանելի են տարբեր խոցելիությունների բիզնես ռիսկերի ցուցադրման միջոցով:

Red Team -ի վարժությունները փորձում են ցուցաբերել բազմակողմանի մոտեցում կազմակերպության քաղաքականությունների, գործառույթների և պաշտպանական միջոցների ամբողջ ծավալը՝ բարելավելու կազմակերպչական պատրաստակամությունը և ուսուցումը անվտանգության մասնագետների համար, ինչպես նաև զննելու ներկայիս մակարդակը: Անկախ Red Team -երը կարող են տալ արժեքավոր և նպատակային տեղեկատվություն՝ խոցելիությունների և պաշտպանողական միջոցների արդյունավետության, ինչպես նաև հետագա կիրառվելիք հսկողության միջոցների վերաբերյալ: