Տեղեկատվական պաշտպանության եղանակները և մեթոդները

Տեղեկատվական պաշտպանությունը միջոցառումների, տեխնոլոգիաների և քաղաքականությունների համակցություն է, որը նախատեսված է տվյալների և տեղեկատվության գաղտնիությունը, ամբողջականությունը և հասանելիությունը պաշտպանելու համար: Այն ուղղված է խուսափելու չարտոնված հասանելիությունից, տվյալների կորստից, փոփոխումից կամ վնասումից, ինչպես նաև համակարգերի և ցանցերի անխափան աշխատանքը պահպանելուն:

Տեղեկատվական պաշտպանությունը ներառում է տարբեր մակարդակներում իրականացվող միջոցառումներ, ինչպիսիք են.

1. **Ֆիզիկական պաշտպանությունը** - Դրանք սարքավորումների և տվյալների ֆիզիկական ապահովման միջոցներ են, օրինակ՝ անվտանգության սենյակներ կամ վիդեո մոնիտորինգ:
2. **Տեխնիկական պաշտպանությունը** - Ծրագրային ապահովման և տեխնիկական լուծումներ են, ինչպիսիք են ֆայերվոլները, հակավիրուսային ծրագրերը և տվյալների կոդավորումը:
3. **Կազմակերպչական պաշտպանություն** - Քաղաքականություններ և ընթացակարգեր են, որոնք սահմանում են, թե ինչպես պետք է աշխատակիցները և օգտատերերը վերաբերվեն տվյալներին և տեղեկատվական համակարգերին:
    1. **Օգտագործողի պաշտպանությունը** - Օգտատերերի իրազեկումը և ուսուցումն է անվտանգության ռիսկերի և սպառնալիքների մասին:

Տեղեկատվական պաշտպանությունը հատկապես կարևոր է կազմակերպությունների և անհատների համար, քանի որ այն պաշտպանում է անձնական, ֆինանսական, բիզնես և այլ զգայուն տվյալները՝ ապահովելով նրանց գործունեության անխափանությունը և վստահությունը: Տեղեկատվական պաշտպանությունը ենթադրում է մի շարք միջոցառումներ և տեխնոլոգիաներ, որոնք ուղղված են տվյալների գաղտնիության, ամբողջականության և հասանելիության

ապահովմանը: Ահա հիմնական մեթոդները, որոնք կիրառվում են տեղեկատվական անվտանգության համար.

Գաղտնագրում (Encryption)

Գաղտնագրումը տվյալների կոդավորման գործընթաց է, որի արդյունքում տվյալները դարձվում են անհասկանալի չարտոնված օգտատերերի համար: Միայն համապատասխան դեկոդավորման բանալիով հնարավոր է դառնում տվյալների ընթերցումը: Գաղտնագրումն ապահովում է տվյալների գաղտնիությունը ինչպես փոխանցման, այնպես էլ պահպանման ընթացքում:

Գաղտնագրումը տվյալների անվտանգության ժամանակակից գործելակերպի հիմնաքարն է և առաջարկում է բազմաթիվ առավելություններ, ներառյալ զգայուն տեղեկատվության պաշտպանությունը և տվյալների պաշտպանության ընդհանուր ռազմավարությունների ամրապնդումը: Առավելությունները հասկանալը կարևոր է թվային ակտիվների ապահովման գործում դրա կենսական դերը հասկանալու համար:

- **Գաղտնիության ապահովում.** Այն կանխում է չարտոնված մուտքը՝ պարզ տեքստը վերածելով անընթեռնելի գաղտնագրային տեքստի, ապահովելով տվյալների գաղտնիությունը և նվազեցնելով տվյալների խախտումների վտանգը:

  Համապատասխանություն տվյալների կանոնակարգերին. Տվյալների գաղտնագրումը չափազանց կարևոր է տվյալների պաշտպանության կանոնակարգերին համապատասխանելու համար, ինչպիսիք են GDPR-ը («General Data Protection Regulation է, որը հայերեն նշանակում է «Ազգային տվյալների պաշտպանության կանոնակարգ) և PCI DSS-ը («Payment Card Industry Data Security Standard է, որը հայերեն նշանակում է «Վճարային քարտերի արդյունաբերության տվյալների անվտանգության ստանդարտ): Այն օգնում է բավարարել իրավական պահանջները՝ պաշտպանելու այնպիսի զգայուն տեղեկատվություն, ինչպիսիք են PII-ը («Personally Identifiable Information է, որը հայերեն նշանակում է «Նույնականացման հնարավոր տեղեկատվություն), ֆինանսական գրառումները և առողջական տվյալները:

- **Տվյալների անվտանգ փոխանցում.** Տվյալների գաղտնագրումն

ապահովում է հաղորդակցման ուղիները՝ քողարկելով զգայուն տեղեկատվությունը, որը կարևոր նշանակություն ունի թվային գործարքների, առցանց հաղորդակցության և ամպի վրա հիմնված ծառայությունների համար, որտեղ տվյալները անցնում են ցանցերով և ինտերնետով:

- **Տվյալներ հանգստի պաշտպանության ժամանակ.** Այն պաշտպանում է տվյալները հանգստի ժամանակ, ներառյալ սերվերների, տվյալների բազաների կամ պահեստավորման սարքերի մասին տեղեկությունները: Նման տվյալների գաղտնագրումն ապահովում է դրանց անհասկանալիությունը առանց ապակոդավորման բանալիի, նույնիսկ չարտոնված մուտքի ժամանակ:
- **Սպառնալիքի մեղմացում.** Տվյալների կոդավորումը հզոր կանխարգելիչ է ներքին և արտաքին սպառնալիքների դեմ: Այն նվազեցնում է ներքին սպառնալիքների վտանգը՝ սահմանափակելով չարտոնված մուտքը և ուժեղացնում է պաշտպանությունը արտաքին սպառնալիքներից՝ գաղտնալսված տվյալները դարձնելով անվերծանելի:
- **Տվյալների ամբողջականություն.** Այն նպաստում է տվյալների ամբողջականության պահպանմանը: Այս գործընթացը երաշխավորում է, որ լիազորված օգտվողները, որոնք հագեցած են ճիշտ ապակոդավորման բանալիով, կարող են մուտք գործել սկզբնական տվյալներ՝ չխախտելով դրանց ամբողջականությունը:

Ճկունություն: Տվյալների դիմակավորման այս բազմակողմանի տեխնիկան կիրառելի է տարբեր միջավայրերում, ներառյալ արտադրական և ոչ արտադրական սցենարները, քանի որ այն աջակցում է տվյալների դինամիկ և ստատիկ դիմակավորմանը՝ տվյալների անվտանգության և գաղտնիության համապարփակ ռազմավարությունների համար: ***<u>Մուտքի վերահսկման միջոցներ (Access Control)</u>***

Մուտքի վերահսկման միջոցները սահմանում են, թե ով և ինչ պայմաններում կարող է օգտվել տվյալ համակարգերից և տվյալներից: Դրանք ներառում են.

1. ***Օգտագործողի նույնականացում (Authentication)***: Օգտատիրոջ անձի

հաստատման մեթոդներ, ինչպիսիք են գաղտնաբառերը, կենսաչափական տվյալները (օրինակ՝ մատնահետք, դեմքի ճանաչում) և երկփուլ նույնականացումը:

2. ***Իրավասությունների սահմանում (Authorization):*** Մուտքի մակարդակների սահմանում, երբ օգտատերերը կարող են միայն որոշակի գործողություններ կատարել կամ հասանելիություն ունենալ որոշակի տվյալների:
3. **Դիսկրետ վերահսկում (Discretionary Access Control - DAC**): Օգտագործողը կամ տվյալների սեփականատերը որոշում է, թե ով կարող է մուտք գործել տվյալներին: Օրինակ, ֆայլերի սեփականատերը կարող է սահմանել, թե ովքեր կարող են կարդալ, խմբագրել կամ ջնջել դրանք:
4. **Պարտադիր վերահսկում (Mandatory Access Control - MAC):** Մուտքի իրավունքները սահմանվում են կենտրոնացված քաղաքականություններով և հիմնվում են տեղեկատվության գաղտնիության մակարդակի վրա: Օրինակ, պետական կազմակերպություններում հաճախ կիրառվում է այս մոտեցումը՝ տվյալների պաշտպանության համար:
5. ***Դերերի վրա հիմնված վերահսկում (Role-Based Access Control - RBAC***): Մուտքի իրավունքները սահմանվում են օգտատերերի դերերի հիման վրա: Յուրաքանչյուր դեր ու նի իր սահմանափակումներն ու թույլտվությունները, և օգտատերերին տրվում են այդ իրավունքները՝ ըստ նրանց զբաղեցրած պաշտոնի կամ դերի:
6. **Երկֆակտոր և բազմաֆակտոր նույնականացում (Two-Factor and Multi-Factor Authentication):** Այս մոտեցումները ապահովում են ավելի բարձր մակարդակի անվտանգություն՝ պահանջելով միաժամանակ մի քանի նույնականացման միջոցներ, օրինակ՝ գաղտնաբառ և կենսաչափական տվյալներ:

7. **Հաշվետվություն և մոնիտորինգ (Logging and Monitoring)**: Բոլոր մուտքերը և գործողությունները գրանցվում են՝ հետագա ստուգման և չարտոնված գործողությունների հայտնաբերման համար:

Մուտքի վերահսկման գործնական օրինակներ

Կառավարական կամ ֆինանսական հաստատություններում կիրառվում են պարտադիր վերահսկման համակարգեր՝ բարձր մակարդակի գաղտնիություն ապահովելու համար: Արտադրական և տեխնոլոգիական ընկերություններում կիրառվում են դերերի վրա հիմնված վերահսկման համակարգեր, որտեղ տարբեր պաշտոններ ունեն տարբեր հասանելիության մակարդակներ:

Կենսաչափական մուտք: Օրինակ, մատնահետքի կամ դեմքի ճանաչման տեխնոլոգիաները ապահովում են բարձր մակարդակի անվտանգություն անձնական կամ կազմակերպչական սարքերում:

Կարևորությունը

Մուտքի վերահսկումը թույլ է տալիս կազմակերպություններին և անհատներին պաշտպանել իրենց տվյալները չարտոնված մուտքից, նվազեցնել խոցելիությունները և պաշտպանել զգայուն տեղեկատվությունը տարբեր սպառնալիքներից:

Ֆայերվոլներ (Firewalls)

Ֆայերվոլները ծրագրային կամ սարքավորողական լուծումներ են, որոնք վերահսկում են ցանցի մուտքը և ելքը՝ կանխարգելելով չարտոնված մուտքը կամ վնասակար գործունեությունը: Դրանք գործում են որպես պատ, որը պահպանում է ցանցի անվտանգությունը:

Հակավիրուսային ծրագրեր (Antivirus Software)

Հակավիրուսային ծրագրերը նախատեսված են վնասակար ծրագրերի հայտնաբերման և դրանց չեզոքացման համար: Դրանք ստուգում են համակարգը և կանխարգելում վիրուսների, տրոյանների և այլ վնասակար ծրագրերի ներթափանցումը:

Ահա մի քանի հայտնի հակավիրուսային ծրագրեր (Antivirus Software)՝

1. Norton Antivirus
2. McAfee Antivirus
3. Kaspersky Antivirus
4. Bitdefender Antivirus
5. Avast Antivirus
6. AVG Antivirus
7. ESET NOD32 Antivirus
8. Trend Micro Antivirus
9. Sophos Antivirus
10. Windows Defender (Microsoft-ի համատեղ առաջարկվող ծրագրում):

Տվյալների պահուստավորում (Data Backup)

Տվյալների պարբերաբար պահուստավորումը կարևոր միջոց է տվյալների վերականգնման համար՝ կորստի կամ վնասման դեպքում: Պահուստային տվյալները պետք է պահպանվեն տարբեր վայրերում, ինչպես տեղական, այնպես էլ ամպային սերվերներում:

Կենսաչափական միջոցառումներ (Biometric Security) Կենսաչափական միջոցառումները օգտագործում են մարդու ֆիզիկական հատկությունները՝ օգտատիրոջ նույնականացման համար: Դրանք ներառում են մատնահետքի, աչքի ցանցաթաղանթի կամ ձայնի նույնականացումը, որոնք ավելի բարձր մակարդակի անվտանգություն են ապահովում:

Հաշվետվություն և մոնիտորինգ (Logging and Monitoring)

Համակարգերի մշտական մոնիտորինգը և գործողությունների գրանցումը (լոգավորումը) թույլ է տալիս հետևել օգտատերերի գործողություններին և հայտնաբերել չարտոնված գործողությունները: Հաշվետվությունների պարբերական ստուգումը օգնում է հայտնաբերել խոցելիությունները և կանխարգելել հնարավոր սպառնալիքները:

Օպերացիոն համակարգերի և ծրագրերի թարմացում (Software Updates and Patch Management)

Օպերացիոն համակարգերի և ծրագրերի պարբերական թարմացումները և դրանցում խոցելիությունների վերացումը կարևոր են անվտանգության ապահովման համար: Թարմացումների միջոցով ուղղվում են հայտնաբերված խոցելիությունները, որոնք կարող են օգտագործվել կիբեռհարձակումների ժամանակ:

Կրթություն և իրազեկություն (Training and Awareness)

Տեղեկատվական անվտանգության հիմնական գործոններից մեկը նաև աշխատակիցների և օգտատերերի իրազեկության բարձրացումն է: Կրթության միջոցով մարդիկ սովորում են, թե ինչպես պաշտպանել իրենց տվյալները և ճանաչել սպառնալիքները, օրինակ՝ ֆիշինգ հարձակումները:

Այս միջոցները, կիրառվելով համակցված ձևով, ապահովում են տվյալների պաշտպանվածությունը: