Տեղեկատվական անվտանգության սպառնալիքների վերլուծություն

Տեղեկատվական անվտանգության սպառնալիքները գործողություններ կամ իրադարձություններ են, որոնք կարող են վտանգել տվյալների և համակարգերի, ամբողջականությունը կամ հասանելիությունը: Այս սպառնալիքները կարող են ծագել տարբեր աղբյուրներից, ինչպիսիք են անհատները, խմբերը կամ նույնիսկ բնական աղետները:

Տեղեկատվական անվտանգության ոլորտում հիմնական սպառնալիքներն ու ռիսկերը վերաբերում են այն վտանգներին, որոնք սպառնում են տվյալների անվտանգությանը և կարող են առաջացնել վնաս կամ խափանում: Ահա դրանցից հիմնականները.

1. Կիբեռհարձակումներ

Վիրուսներ և վնասակար ծրագրեր (Malware): Վնասակար ծրագրերը, ինչպիսիք են վիրուսները, ճիճուները, տրոյանները և ransomware-ները, կարող են վնասել համակարգչային համակարգերին, խափանել տվյալների հասանելիությունը կամ դրանց ամբողջականությունը: Կիբերհարձակումները թույլ են տալիս շարքից դուրս բերել արդյունաբերական կառույցները: Համաձայն Կասպերսկու լաբորատորիայի հրապարակած տվյալների՝ 2016թ.- ին համաշխարհային արդյունաբերական ողջ համակարգի 27,5% - ում հայտնաբերվել են վնասակար ծրագրեր:[1] Այս ոլորտում առանձնապես վտանգավոր են հարձակումները միջուկային ենթակառուցվածքների վրա: Օրինակ, հատկանշական է, որ ինչպես 1986թ. Չեռնոբիլի, այնպես էլ ավելի ուշ՝ 2011թ. Ճապոնական Ֆուկուսիմա-1 ԱԷԿ-ներում պա տահած վթարների պատճառը, համաձայն որոշ վարկածների[2], այլ երկրների կողմից կատարված նպատակաուղղված գործողություններն են: Ինչպես տեսնում ենք, կիբեռհարձակումները դարձել են տարածված երևույթ, և տրամաբանական է, որ ընձեռված հնարավորություններից լայնորեն օգտվում են նաև քաղաքական ոլորտում:

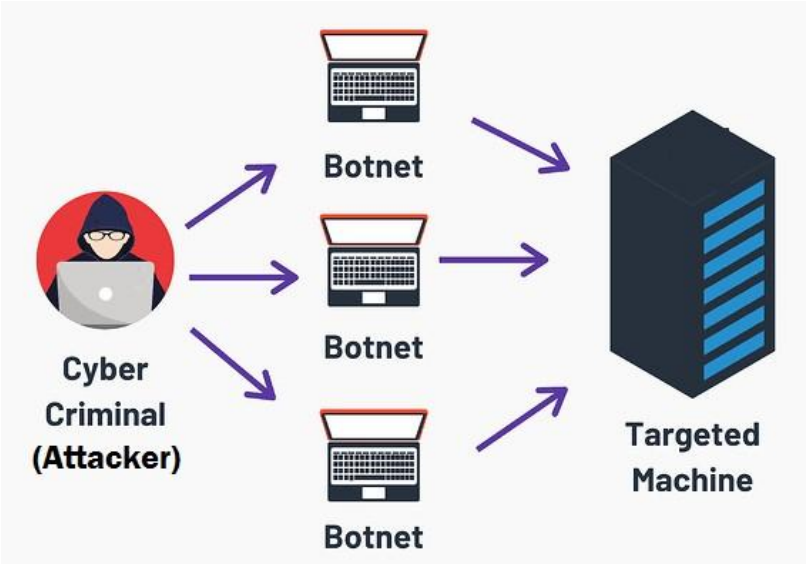
[1] http://www.kaspersky.ru/

[2] Катастрофа в Чернобыле была организована, чтобы ударить по СССР, http://www.km.ru/v-rossii/2017/03/24/798483-katastrofa-v-chernobyle-byla-organizovanachtoby-udarit-po-sssr

2. **Ֆիշինգ (Phishing):** Սա խաբեբայության ձև է սոցիալական ինժեներական հարձակում է, որը փորձում է խաբել օգտատերերին՝ բացահայտելու զգայուն տեղեկություններ, ինչպիսիք են օգտանունները, գաղտնաբառերը կամ վարկային քարտի տվյալները: Օգտագործողները մոլորեցվում են տրամադրում իրենց անձնական կամ ֆինանսական տվյալները՝ կեղծ կայքերի կամ էլ. նամակների միջոցով:

Ֆիշինգի նամակները կամ հաղորդագրությունները սովորաբար օրինական աղբյուրից են, օրինակ՝ բանկից կամ վարկային քարտերի ընկերությունից:

- **DDoS (Distributed Denial of Service) հարձակումներ:** Այս հարձակումները ստեղծում են համակարգի կամ ցանցի գերբեռնվածություն, որն առաջացնում է կայքի կամ ծառայության խափանումներ, փորձում են համակարգը ծանրաբեռնել երթևեկությամբ՝ այն անհասանելի դարձնելով օրինական օգտատերերի համար: DDoS հարձակումները կարող են շատ խանգարել և կարող են հանգեցնել զգալի ֆինանսական կորուստների:



2. Սոցիալական ինժեներիա

Սոցիալական ինժեներիան տեխնիկա է, որի միջոցով հարձակվողները փորձում են մարդկանց մոլորեցնել և ստանալ նրանց գաղտնի տվյալները՝ օգտագործելով վստահություն ներշնչող միջոցներ կամ այլ մեթոդներ: Օրինակ՝ սուտ զանգերը, երբ հարձակվողը ներկայանում է որպես օգտատիրոջ ընկեր կամ աշխատակից:

3. Համակարգային խոցելիություններ

Համակարգերի կամ ծրագրային ապահովման թերությունները հաճախ օգտագործվում են կիբեռհանցագործների կողմից՝ չարտոնված մուտքի կամ տվյալների փոփոխության համար: Խոցելիությունները կարող են լինել սխալ ծրագրային կոդի, անվտանգության թույլ կարգավորումների կամ հնացած ծրագրերի պատճառով:

4. Ներքին սպառնալիքներ

Ներքին սպառնալիքները գալիս են կազմակերպության ներսից՝ աշխատակիցների կամ այլ ներսում գտնվող անձանց կողմից: Դրանք կարող են լինել կամ դիտավորյալ վնաս հասցնելու նպատակով, կամ չիմացության կամ անփութության հետևանքով: Օրինակ՝ գաղտնի տվյալների պատահական արտահոսքը կամ չպաշտպանված սարքավորումների օգտագործումը:

5. Տվյալների արտահոսք

Տվյալների արտահոսքը կարող է տեղի ունենալ ինչպես արտաքին, այնպես էլ ներքին սպառնալիքների պատճառով: Սա հաճախ առաջանում է անվտանգության թույլ միջոցների կամ չարտոնված հասանելիության արդյունքում և կարող է հանգեցնել զգայուն տվյալների բացահայտմանը:

6. Ընդլայնված կայուն սպառնալիքներ (APTs). Բարձր նպատակային հարձակումներ, որոնք իրականացվում են հմուտ հարձակվողների կողմից, ովքեր վճռական են մուտք գործել համակարգ և երկար ժամանակ աննկատ մնալ: APT-ները սովորաբար օգտագործվում են զգայուն տեղեկատվություն գողանալու կամ կարևորենթակառուցվածքը խափանելու համար:

7. Մարդկային սխալներ

Մարդկային սխալները հաճախ հանդիսանում են անվտանգության խնդիրների աղբյուր: Օրինակ՝ սխալ ֆայլերի կամ տվյալների փոխանակումը, թույլ և հեշտ կռահելի գաղտնաբառերի օգտագործումը կամ տվյալների անզգույշ մուտքը:

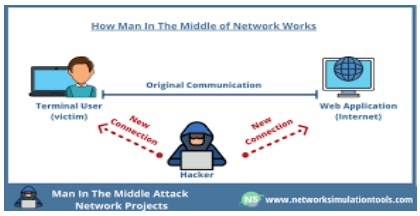
8. Ֆիզիկական սպառնալիքներ

Ֆիզիկական սպառնալիքները ներառում են այնպիսի իրավիճակներ, երբ համակարգիչները, սերվերները կամ այլ սարքավորումներ կարող են վնասվել բնական աղետների, գողության կամ վանդալիզմի հետևանքով: Ֆիզիկական անվտանգության միջոցները նախատեսված են պաշտպանելու սարքավորումները և դրանցում գտնվող տվյալները:

9. Ռիսկերի վերլուծություն և կառավարում

Ռիսկե րը կառավարման ենթակա են միայն այն դեպքում, երբ կան հստակ ռազմավարություններ և միջոցառումներ դրանց դեմ: Ռիսկերի վերլուծությունը ներառում է սպառնալիքների ճանաչումը, խոցելիությունների բացահայտումը և դրանցից բխող վտանգների գնահատումը՝ համապատասխան միջոցներ ձեռնարկելու նպատակով:

10. Man-in-the-Middle (MitM) հարձակումներ. հարձակումներ, որոնք գաղտնալսում են երկու կողմերի միջև հաղորդակցությունը՝ գաղտնի տեղեկատվություն գողանալու նպատակով: MitM հարձակումները կարող են իրականացվել ինչպես լարային, այնպես էլ անլար ցանցերում:



Այս սպառնալիքներն ու ռիսկերը ցույց են տալիս, թե որքան կարևոր է տեղեկատվական անվտանգության ապահովումը ինչպես անհատական, այնպես էլ կազմակերպչական մակարդակներում:

Գտնվելով աշխարհաքաղաքական բարդ տարածաշրջանում և ներքաշված լինելով տարաբնույթ տեղեկատվական ակտիվ ներազդեցությունների և ներհոսքերի մեջ՝ Հայաստանի Հանրապետությունը այսօր կարևորագույն խնդիր ունի նվազագույնի հասցնել տեղեկատվական ոլորտում պետության ազգային շահերին սպառնացող վտանգների բացասական միտումները: Որպես տեղեկատվական ոլորտի սպառնալիք կարելի է առանձնացնել հեռահաղորդակցային համակարգերի բնականոն գործունեության միջոցների թույլ պաշտպանվածությունը, չթույլատրված մուտքերի հնարավորությունը, հեռահաղորդակցության ոլորտում մենաշնորհային դիրքի ամրագրումը, անօրինական կարգով տրամադրված տեղեկատվությունը և այլն: Պետության տեղեկատվական անվտանգության սպառնալիքները, ըստ ընդհանուր ուղղվածության, դասակարգվում են հետևյալ տիպերի.

1. սպառնալիքներ՝ ուղղված երկրի պետական քաղաքականության տեղեկատվական ապահովմանը,
2. սպառնալիքներ՝ ուղղված հայրենական տեղեկատվական ռեսուրսների զարգացմանը, արտադրանքի ներքին շուկայի բավարարմանը և համաշխարհային շուկա արտահանմանը, ինչպես նաև հայրենական տեղեկատվական միջոցների կուտակման, պահպանման և արդյունավետ օգտագործման ապահովմանը,
3. սպառնալիքներ՝ ուղղված երկրի տեղեկատվական և հեռահաղորդակցային ռեսուրսների և համակարգերի անվտանգությանը[3]:

[3] Վ.Կ.Աթոյան, Տեղեկատվական-հաղորդակցական անվտանգության ապահովման արդի խնդիրների շուրջ, 2015թ., էջ 91: