**Կիբեռանվտանգության միջոցառումներ**

“Պահապան Արծիվ”ը օգտագործում է կիբեռանվտանգության տարբեր միջոցներ՝ բիզնեսի տվյալները, դրամական միջոցների հոսքը և հաճախորդներին առցանց անվտանգ պահելու համար: Այս միջոցները ուղղված են տարբեր աղբյուրներից առաջացող ռիսկերի կանխմանը, այդ թվում՝

ինտերնետային հարձակումներ, օրինակ՝ լրտեսող ծրագրեր կամ չարամիտ ծրագրեր

օգտատերերի կողմից առաջացած թույլ կողմերը, օրինակ՝ հեշտությամբ գուշակվող գաղտնաբառերը կամ սխալ տեղաբաշխված տեղեկատվությունը

համակարգի կամ ծրագրային ապահովման բնորոշ թերություններ և խոցելիություններ

տապալել համակարգի կամ ծրագրային ապահովման առանձնահատկությունները։

Կիբեռանվտանգության միջոցները

Տեղադրված է համակարգերում գաղտնաբառերի ուժեղության ենթահամակարգը

Օգտագործվում է մեծատառ և փոքրատառ տառերի, թվերի և նշանների համադրություն

Այն ութից մինչև 12 նիշ է

Խուսափում ենք անձնական տվյալների օգտագործումից պարբերաբար փոխելով այն

Երբեք այն չի օգտագործվում մի քանի օգտատերերի համար

Օգտագործում ենք նաև երկու գործոն վավերացում

ՈՒղեցույց։

“ Ստեղծեք գաղտնաբառի քաղաքականություն ձեր բիզնեսի համար՝ օգնելու անձնակազմին հետևել անվտանգության լավագույն փորձին: Փնտրեք տարբեր տեխնոլոգիական լուծումներ՝ ձեր գաղտնաբառի քաղաքականությունը կիրառելու համար, օրինակ՝ պլանավորված գաղտնաբառի վերակայում: Գաղտնաբառերի վերաբերյալ մանրամասն ուղեցույցի համար կարդացեք Կիբերանվտանգության ազգային կենտրոնի (NCSC) ուղեցույցը ձեր տվյալները պաշտպանելու համար գաղտնաբառերի օգտագործման վերաբերյալ և հաշվի առեք տարբեր գաղտնաբառերի ռազմավարություններ, որոնք կարող են բարձրացնել ձեր բիզնեսի անվտանգությունը: “

Վերահսկում ենք տվյալների և համակարգերի հասանելիությունը

Օգտատերերը կարող են մուտք գործել միայն տվյալներ և ծառայություններ, որոնց համար նրանք լիազորված են:

Վերահսկում ենք ֆիզիկական մուտքը տարածքներ և համակարգչային ցանց

սահմանափակում մուտքը չարտոնված օգտվողներին։

սահմանափակում ենք տվյալների կամ ծառայությունների հասանելիությունը հավելվածների վերահսկման միջոցով, սահմանափակում այն, ինչ կարելի է պատճենել համակարգից և պահել արտաքին սարքերում։

Սահմանափակում ենք որոշ տեսակի էլփոստի հավելվածների ուղարկումն ու ստացումը։

Օգտագործում ենք անվտանգության ծրագրակազմ, ինչպիսիք են հակալրտեսող ծրագրերը, հակավիրուսային և հակավիրուսային ծրագրերը, որոնք օգնում են հայտնաբերել և հեռացնել վնասակար ծածկագիրը, եթե այն գտնվի մեր ցանցում:

Պարբերաբար թարմացնում ենք ծրագրերը և համակարգերը

Թարմացումները պարունակում են անվտանգության կարևոր թարմացումներ, որոնք օգնում են պաշտպանվել հայտնի վրիպակներից և խոցելիությունից: Համոզվում ենք , որ արդի ենք պահում մեր ծրագրաշարը և սարքերը, որպեսզի խուսափեք հանցագործների զոհը դառնալուց։

Օգտագործում ենք ներխուժման դետեկտորները, համակարգերը և ցանցի անսովոր գործունեությունը վերահսկելու համար: Եթե հայտնաբերման համակարգը կասկածում է անվտանգության պոտենցիալ խախտման մասին, այն ահազանգ է տալիս:

Իրազեկությունը բարձր մակարդակի վրա է։ Մեր աշխատակիցները պատասխանատվություն են կրում մեր բիզնեսի անվտանգությունն ապահովելու հարցում: Համոզված ենք, որ նրանք հասկանում են իրենց դերը և ցանկացած համապատասխան քաղաքականություն և ընթացակարգ, և նրանց տրամադրում ենք կիբերանվտանգության կանոնավոր իրազեկում և ուսուցում: