KASPERSKY lab

ՏՏ ԱՆՎՏԱՆԳՈՒԹՅՈՒՆԸ «ԹԵՅՆԻԿՆԵՐԻ» ՀԱՄԱՐ

Ջորջինա Գիլմոր, Պիտեր Բիդմոր

«Կասպերսկու լաբորատորիայի» մասին

«Կասպերսկու լաբորատորիան» ինֆորմացիոն անվտանգության ոլորտում դինամիկ զարգացող կազմակերպություններից է: Այն տվյալ ոլորտի առաջատար քառյակի մեջ է մտնում: «Կասպերսկու լաբորատորիան» գոյություն ունի արդեն 15 տարի և այսքան ժամանակ SS անվտանգության բնագավառի նորարարներից է, մշակում է պաշտպանական արդյունավետ լուծումներ մեծ, փոքր և միջին կազմակերպությունների և սովորական օգտատերերի համար: Այժմ «Կասպերսկու լաբորատորիան» գործում է ավելի քան 200 երկրում՝ պաշտպանելով ավելի քան 300 միլիոն օգտատերերի ամբողջ աշխարհում:

Մանրամասն տես՝ www.kaspersky.ru/business

ՏՏ ԱՆՎՏԱՆԳՈՒԹՅՈՒՆԸ «ԹԵՅՆԻԿՆԵՐԻ» ՀԱՄԱՐ

Տպագրված է «Կասպերսկի Լաբորատորիա»-ի կողմից, սահմանափակ տպաքանակ

ՆԵՐԱԾՈՒԹՅՈՒՆ

Ձեզ ողջունում է «SS անվտանգությունը սկսնակների համար» գիրքը: Գրքում ներկայացվում են ինֆորմացիոն անվտանգության մի քանի խնդիրներ, որոնց առնչվում են կազմակերպությունները համացանցում: Այն խորհուրդները, որոնք դուք կգտնեք այս գրքում, կօգնեն ձեզ պաշտպանել ձեր կազմակերպության գաղտնի տեղեկատվությունը և այսպիսով խուսափել օրենսդրական և իրավական պատժամիջոցներից և պահպանել գործարար բարձր վարկանիշը:

Վերջին տասնամյակում համակարգչային տեխնոլոգիաների սրընթաց աճը օգնել է կազմակերպություններին կրճատել ծախսերը, բարձրացնել հաճախորդների սպասարկման արդյունավետությունը և որակը: Միևնույն ժամանակ նույն տեխնոլոգիաները հնարավորություն են տվել ցանցահեներին հարձակումներ գործելու համար:

Այսօր բոլոր կազմակերպությունները (նույնիսկ նրանք, որոնք գտնում են, որ չունեն գաղտնի տեղեկատվություն, որը պետք է պաշտպանել) պետք է իմանան SS անվտանգության վտանգների և դրանցից պաշտպանվելու մասին: Այդ նպատակով է գրվել այս գիրքը:

ԱՅՍ ԳՐՔԻ ՄԱՍԻՆ

Չնայած փոքր ծավալին, գիրքը պարունակում է օգտակար տեղեկություններ, որոնք կօգնեն զարգացող կազմակերպություններին ընտրել գաղտնի ինֆորմացիան, այդ թվում հաճախորդների տվյալները, պաշտպանելու լավագույն ճանապարհները, պաշտպանել համակարգիչները և բջջային սարքերը վիրուսներից, վնասատու հարձակումներից և այլ վտանգներից:

Բոլոր մեծ և փոքր կազմակերպությունները, առանց բացառության, կարող են թիրախ դառնալ ցանցահենների համար, ովքեր կատարելագործված մեթոդներով կարող են մուտք գործել համակարգչի մեջ և կորզել գաղտնի ինֆորմացիա, իսկ բանկային հաշիվներից՝ գումար: Այսպիսի իրավիճակում միջազգային խոշոր կազմակերպությունները կարող են վարձել ինֆորմացիոն անվտանգության փորձագետների, իսկ փոքր կազմակերպությունները չունեն այդ փորձագետներին: «SS անվտանգությունը սկսնակների համար» գիրքը օգնություն է կազմակերպություններին, որտեղ ուշադրություն է դարձվում հետևյալ հարցերին՝

- *Ինչու՞ է պետք պաշտպանել անձնական այն տեղեկատվությունը, որին տիրապետում է կազմակերպությունը,*
- *ինֆորմացիոն անվտանգության արդիական ռիսկերի սպեկտրը և բնույթը,*
- *գաղտնի ինֆորմացիայի պաշտպանման պարզ միջոցներ՝ առանց ավելորդ ծախսերի,*
- *կազմակերպության ինֆորմացիոն անվտանգությունը էապես բարձրացնող հարմար միջոցներ:*

ՀԱՄԱՐՁԱԿ ԵՆԹԱԴՐՈՒԹՅՈՒՆՆԵՐ

Մենք հուսով ենք, որ այս գրքում դուք կգտնեք ձեզ համար արժեքավոր ինֆորմացիա, այդ պատճառով արել ենք մի քանի ենթադրություն՝

- *ընկերությունը, որը դուք ղեկավարում եք կամ որտեղ աշխատում եք, օգտագործում է նոութբուքեր, համակարգիչներ կամ բջջային սարքեր,*
- *դուք ուզում եք համոզված լինել, որ կազմակերպությունը պահպանում է ինֆորմացիոն անվտանգության կանոնները,*
- *ձեզ համար կարևոր է ապահովել բիզնես-տվյալների գաղտնիությունը,*
- *դուք ուզում եք իմանալ՝ ինչպես խուսափել ցանցահեների հարձակումից,*
- *դուք դիտարկում եք որոշակի բիզնես-տվյալների պահպանումը ամպի մեջ,*
- *դուք ցանկանում եք ստանալ խորհրդատվություն կազմակերպության ինֆորմացիոն համակարգի պաշտպանության ծրագրային ապահովման ընտրության հարցում:*

ԻՆՉՊԵՍ Է ԿԱԶՄՎԱԾ ԱՅՍ ԳԻՐՔԸ

Գիրքը բաղկացած է վեց գլխից, որոնք պարունակում են հագեցած տեղեկատվություն:

→ ***Գլուխ 1. Ինչու կազմակերպությունը պետք է պաշտպանի գաղտնի տեղեկատվությունը:*** *Մենք բացատրում ենք, թե ինչու է վտանգավոր թվացյալ անվտանգությունը:*

→ ***Գլուխ 2. Ինչ է պետք հենց ձեր կազմակերպությանը:*** *Անվտանգությունը անհրաժեշտ է բոլոր կազմակերպություններին, բայց անվտանգության պահանջները տարբեր են:*

→ ***Գլուխ 3. Ողջ ճշմարտությունը անվտանգության վտանգների մասին:*** *Դուք կիմանաք, թե ինչու ժամանակակից SS համակարգերը բարդացել են, իսկ բիզնեսի խոցելիությունը ավելի մեծացել:*

→ ***Գլուխ 4. Ինֆորմացիոն անվտանգության մակարդակի բարձրացման պլանավորում:*** *Գնահատեք գոյություն ունեցող ռիսկերը և մշակեք դրանցից պաշտպանվելու մարտավարություն: Մենք կբացատրենք, թե ինչին պետք է ուշադրություն դարձնել տեղեկատվությունը «ամպի մեջ» պահելիս:*

→ ***Գլուխ 5. Պաշտպանական ճիշտ համակարգի ընտրություն:*** *Մենք կխոսենք այն գործոնների մասին, որոնք կօգնեն ճիշտ ընտրություն կատարել ժամանակակից շուկայում ներկայացված արտադրանքից:*

→ ***Գլուխ 6. 10 հարց, որոնք կօգնեն ձեզ:*** *Տվեք այդ հարցերը կողմնորոշվելու համար:*

ՕԳՏԱԳՈՐԾՎՈՂ ՆՇԱՆԱԿՈՒՄՆԵՐ

Անհրաժեշտ տեղեկությունը հեշտությամբ գտնելու համար գրքում կարևոր տեղեկության կողքին դրված են հատուկ նշաններ:

Պետք է ուշադրություն դարձնել կարևոր խորհրդին:

Պետք է հիշել կարևոր տեղեկությունը:

Ուշադրություն դարձրեք հնարավոր դժվարություններին:

ՈՐ ԳԼՈՒԽԸ ԿԱՐԴԱԼ ՍԿԶԲԻՑ

Գիրքը կարդացվում է հեշտությամբ և արագ: Ձեր ընտրությամբ կարող եք որոշել, թե որ գլուխը կարդալ սկզբից: Մենք վստահ ենք, որ դուք կգտնեք արժեքավոր խորհուրդներ ձեր հաճախորդների տվյալների և կարևոր այլ տեղեկատվության պաշտպանության համար:

Գլուխ 1

ԻՆՉՈՒ ՅԱՆԿԱՑԱԾ ԿԱԶՄԱԿԵՐՊՈՒԹՅՈՒՆ ՊԵՏՔ Է ՊԱՇՏՊԱՆԻ ԳԱՂՏՆԻ ԻՆՖՈՐՄԱՑԻԱՆ

Այս գլխում՝

- *Ոչ մեծ կազմակերպությունների լրացուցիչ ռիսկերի գնահատում:*
- *Արժեքավոր բիզնես-ինֆորմացիայի պաշտպանություն:*
- *Ինչպես խուսափել վտանգներից թվացյալ պաշտպանվածության դեպքում:*
- *Ինչու ցանկացած կազմակերպություն կարող է դառնալ կիբեռհանցագործների զոհը:*

Առաջին գլխում մենք կդիտարկենք կազմակերպությունների համար ինֆորմացիոն անվտանգության մի քանի ռիսկեր և կբացատրենք, թե ինչու պաշտպանության խնդիրը չպետք է մղել երկրորդ պլան:

ԿԱԶՄԱԿԵՐՊՈՒԹՅՈՒՆՆԵՐԸ ՎՏԱՆԳՎԱԾ ԵՆ

Տեղեկատվական մեր ժամանակներում գիտելիքը ոչ միայն ուժ է, այլ ավելին է: Ձեր կազմակերպության հաջողությունը կախված է այն տեղեկությունից, որ այն պահպանում է՝ լինի դա նորարարության մասին, արտադրանքի մասին կամ հաճախորդի մասին: Կազմակերպության համակարգված աշխատանքը կարող է խաթարվել, եթե պահպանվող տեղեկությունները դառնան անհասանելի: Ցանկալի չէ, որ այդ

տեղեկությունները հայտնվեն չարագործների ձեռքում: Եթե կազմակերպության տեղեկատվական բազան պաշտպանված չէ, ապա ցանցահենները հեշտությամբ կարող են գողանալ այնտեղ պահվող ինֆորմացիան, համացանցի միջոցով ղեկավարել կազմակերպության ֆինանսական հաշիվները:

Ցավոք սրտի ցանկացած մեծության կազմակերպություն կարող է ցանցահենների համար թիրախ դառնալ: Նրանք տիրապետում են տարբեր մեթոդների, որոնցով կարող են խաթարել կազմակերպության բիզնես գործընթացը, կորզել գաղտնի տեղեկությունները, գողանալ կորպորատիվ հաշիվները: Շատ հաճախ նման հարձակումների զոհերը իմանում են խնդրի մասին այն ժամանակ, երբ արդեն ուշ է:

Կիբեռհանցագործությունները և կիբեռհանցագործները

Հանցագործներին միշտ հաջողվում է գտնել այն բացը, որն առկա է պաշտպանության համակարգում: Համատարած համացանցի դարում ձևավորվել է հանցագործների նոր տեսակ՝կիբեռհանցագործներ:

Կիբեռհանցագործություն են համարվում ինֆորմացիոն համակարգերի և համացանցի միջոցով կատարվող մի շարք հակաօրինական գործողությունները: Շատ կազմակերպություններ անտեսում են նման վտանգները, իսկ հանցագործները օգտվում են դրանից:

Կիբեռհանցագործները համակարգիչները խոցելու, գաղտնի ինֆորմացիա կորզելու և փող գողանալու համար մշակում են բարդ մեթոդներ, ինչը վկայում է նրանց բարձր որակավորման մասին: Կիբեռհանցագործների հասցրած ֆինանսական վնասը կարող է հասնել մեծ չափերի, իսկ հանցագործություն կատարելու համար ավելի քիչ միջոցներ են ծախսվում: Այդ պատճառով էլ կիբեռհանցագործությունը շարունակում է աճել:

ՓՈՔՐ ԿԱԶՄԱԿԵՐՊՈՒԹՅՈՒՆԸ ԵՆԹԱԿԱ Է ՌԻՍԿԵՐԻ

Ամենօրյա աշխատանքում փոքր կազմակերպությունների համար առկա են նույն խնդիրները, ինչ որ մեծ կազմակերպությունների համար: Բոլոր կազմակերպությունները անընդհատ ստիպված են հարմարվել շուկայի փոփոխվող պայմաններին, արձագանքել մրցակիցների գործողություններին և մի քայլ առաջ կռահել հաճախորդների պահանջները և նախընտրությունները: Բացի այս բոլոր գործոններից, փոքր բիզնեսը ստիպված է լուծել մի շարք խնդիրներ, որոնք ծագում են կազմակերպության զարգացմանը զուգահեռ, օրինակ՝

- *աճող պահանջարկը բավարարելու համար վարձել նոր աշխատողներ և սովորեցնել նրանց,*
- *փնտրել ավելի մեծ մակերեսով տարածքներ և կազմակերպության տեղափոխումը իրականացնել առանց ամենօրյա աշխատանքի ընդհատման,*
- *լրացուցիչ ֆինանսավորման հայթայթում՝ բիզնեսի զարգացման համար,*
- *բացել նոր գրասենյակներ,*
- *բիզնես-պրոցեսների համակարգում, օրինակ՝ հաճախորդների տվյալների պաշտպանում:*

Բոլոր այս քայլերը անհրաժեշտ են կազմակերպության արդյունավետ կառավարման և հետագա զարգացման համար:

Սա իմ խնդիրը չէ

Զարգացող կազմակերպությունների հիմնադիրները և աշխատակիցները լուծում են տարբեր խնդիրներ: Հաճախ փոքր ձեռնարկության մի աշխատակից կամ մի քանի համախոհներ կատարում են մի քանի պարտականություն: Այդպիսի կազմակերպությունում սովորաբար չկա կադրերի բաժին, իրավաբանական և SS անձնակազմ:

Եթե դուք ուզում եք, որ ձեր բիզնեսը զարգանա, դուք և ձեր գործընկերները պետք է կենտրոնանաք բիզնես-պրոցեսի վրա և տիրապետեք պրոցեսի նրբություններին:

Կարելի է ժամավճարով վարձել որակավորված մասնագետների, բայց դա թանկ հաճույք է: Կազմակերպության նպատակային գործունեության համար ծախսված յուրաքանչյուր դրամը պակասեցնում է ներդրումները մյուս կարևոր բնագավառներում և կարող է դանդաղեցնել բիզնեսի զարգացումը:

Ո՞րն է ինֆորմացիոն տեխնոլոգիաների առանձնահատկությունը

Կազմակերպությունները չեն կարող գործել՝ չօգտագործելով SS գոնե հիմնական տարրերը, օրինակ՝ նոութբուքերը: SS-ն միջոց է, որով հնարավոր է հասնել նպատակին, այն կարևոր օղակ է, որը հնարավորություն է տալիս բարձրացնել բիզնեսի արդյունավետությունը և լավացնել փոխգործակցությունը հաճախորդների, աշխատակիցների և մատակարարների հետ: SS համակարգերը պետք է ծառայեն բիզնեսին, նշանակում է նրանց համալարումը և կառավարումը պետք է լինի պարզ: Կազմակերպության համակարգիչները և գաղտնի տեղեկատվությունը պաշտպանող SS ծրագրերը պետք է պարզ և հարմար լինեն օգտագործելու համար:

Եթե գործում են ջունգլիների օրենքները՝ մտածեք ձեր պաշտպանվածության մասին

Կազմակերպությունները, որոնք համակարգիչները համարում են անխուսափելի չարիք, նույն կերպ են վերաբերվում դրանցում պահվող ինֆորմացիայի պաշտպանությանը: Նման վերաբերմունքը հասկանալի է, եթե տեղեկատվական տեխնոլոգիաները ձեզ համար դյուրըմբռնելի չեն:

Փաստն այն է, որ գործարար ինֆորմացիայի անվտանգությունը շատ կարևոր է: Հաշվի առնելով այն հանգամանքը, որ չարագործները օգտագործում են համացանցը կազմակերպությունների համակարգիչները խոցելու համար, կազմակերպությունները պետք է չանտեսեն համակարգիչների անվտանգության խնդիրը:

Երբեմն պաշտպանական մի քանի միջոց բավական է, որ խնայի ձեր նյարդերը և դրամական միջոցները:

SS համակարգերի և տեղեկատվության անվտանգության ապահովումը կարող եք համարել «չարիք», սակայն կիբեռհանցագործները հարձակում են գործում չպաշտպանված համակարգերի վրա:

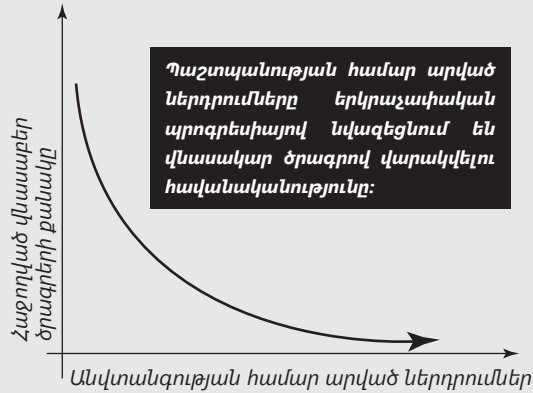
Խանութի տնօրենը երբեք բաց չի թողնի դրամարկղը՝ իմանալով, որ այն կարող են թալանել: Ճիշտ այդպես, յուրաքանչյուր կազմակերպություն, որն օգտագործում է համակարգիչներ, բջջային սարքեր, համացանցը, պետք է ապահովի իր SS համակարգի անխոցելիությունը: Այսօր հեշտությամբ կարելի է դառնալ կիբեռհանցագործների զոհը, որոնք գտնում են համակարգիչների, պլանշետների, սմարթֆոնների պաշտպանական համակարգերի խոցելի տեղերը: Այդ պատճառով պետք է միջոցներ ձեռնարկել գաղտնի տվյալների կամ բանկային հաշիվներից գումարների գողությունը կանխելու համար:

Պաշտպանական նվազագույն գործառույթը մեծ օգուտ է տալիս

Պաշտպանության բացակայության և անվտանգության նվազագույն միջոցների կիրառման միջև կա մեծ տարբերություն: Պաշտպանության նվազագույն միջոցառումները ձեր կազմակերպությունում կիբեռհանցագործներին կստիպեն փնտրել այլ թիրախներ:

Գծանկարում երևում է, որ անվտանգության համար ներդրած նյութական համեստ միջոցները նվազեցնում են վնասատու գրոհի հնարավորությունը:

Պաշտպանության համար արված ներդրումներ



Անվտանգությունը չպետք է խանգարի բիզնեսին

Հանրահայտ ճշմարտություն է՝ ժամանակը փող է: Ավելորդ հոգսերը շեղում են մարդուն իր հիմնական գործից, խլում են նրա ժամանակը, հնարավորությունները և ֆինանսական միջոցները: Արդիական բիզնես-խնդիրներին արագ արձագանքելը և դրանց լուծման շուրջ կենտրոնանալը այն կարևոր հատկություններն են, որոնց շնորհիվ դուք հիմնել եք ձեր կազմակերպությունը: Որքան էլ SS անվտանգությունը կարևոր լինի, այն չպետք է խանգարի, որ դուք հասնեք ձեր բիզնես-նպատակներին:

Ձեր հիմնական գործունեությանը չվերաբերող խնդիրների լուծմանը ժամանակ տրամադրելը խանգարում է մրցակցային առավելությունների մեծացմանը և բիզնեսի զարգացմանը: Ինֆորմացիոն անվտանգությանը ոչ ճիշտ մոտեցումը և պաշտպանական ոչ ճիշտ տեխնոլոգիաները կարող են խանգարել ձեր կազմակերպության զարգացմանը:

Կիբեռհանցագործների դյուրահաս զոհը

Տագնապելով արտադրողականության նվազման համար շատ կազմակերպություններ ուշադրություն չեն դարձնում SS անվտանգությանը: Եթե տարիներ առաջ նման մոտեցումը թույլատրելի էր, ապա այսօրվա կիբեռհանցագործության պայմաններում անթույլատրելի ռազմավարություն է: Քանի որ փոքր կազմակերպությունը ավելի խոցելի է, քան մեծը, պարզ է, որ ձեր կազմակերպության SS անվտանգությունը չի կարելի անուշադրության մատնել:

Գոյություն ունեն պարզ միջոցներ, որոնք կօգնեն ձեր կազմակերպությանը պաշտպանել գաղտնի ինֆորմացիան: Ժամանակակից շուկայում կան ծրագրեր, որոնք մշակված են

փոքր կազմակերպությունների համակարգերի և տվյալների պաշտպանության համար: Այդ լուծումները ապահովում են բիզնեսի SS անվտանգությունը, դրանց տեղադրումը շատ ժամանակ չի պահանջում և այդ ծրագրերը հեշտ է ղեկավարել:

Նույնիսկ խոշոր կազմակերպությունները հնարավոր է չունենան բավարար ռեսուրսներ պաշտպանական համակարգի վրա հարձակումից հետո այն վերականգնելու համար: Իսկ փոքր կազմակերպությունները հնարավոր է նման միջադեպից հետո այլևս չկարողանան շարունակել իրենց գործունեությունը:

ԹՎԱՑՅԱԼ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ՁԳԱՑՈՒՄԸ

Որոշ կազմակերպություններ զգոն չեն՝ մտածելով, որ կիբեռհանցագործները հետաքրքրված են մեծ կազմակերպություններով: «Մենք անհանգստանալու ոչինչ չունենք: Ում է պետք մեր փոքր կազմակերպությունը, եթե կան ավելի մեծ և հարուստ կազմակերպություններ: Մենք կիբեռհանցագործների ցուցակում չկանք», - մտածում է փոքր կազմակերպության տերը:

Կիբեռհանցագործները օգտագործում են սկանավորող զանազան միջոցներ՝ «խելացի» գործիքներ, որոնք համացանցի միջոցով գտնում են այն կազմակերպությունները, որոնց համակարգիչները բավարար չափով պաշտպանված չեն:

Սկաներները մի ակնթարթում գտնում են հաջորդ զոհին և որոշում են նրա խոցելի տեղերը:

Թվում է, թե ֆանտաստիկ ֆիլմի սյուժե է, բայց իրականություն է: Ամեն օր տարբեր բարդ մեթոդներով հարձակումներ են կատարվում փոքր կազմակերպությունների վրա: Մեկ օրվա ընթացքում «Կասպերսկու լաբորատորիան» բացահայտում է վնասատու ծրագրերի կիրառմամբ շուրջ 12000 գրոհ:

Փոքր կազմակերպությունները ավելի հեշտ է գրոհել

Սովորաբար կիբեռհանցագործները ձգտում են քիչ ջանք և կարճ ժամանակ ծախսելով ՝ ստանալ մեծ շահույթ իրենց անօրինական գործողություններից: Միջազգային կորպորացիայի անվտանգության համակարգը կոտրելով կարելի է շատ մեծ շահույթ ստանալ, բայց նման կազմակերպությունների պաշտպանական խոչընդոտները բավականին բարդ են և դրանց մեջ թափանցելը դժվար է: Այդ պատճառով էլ հանցագործները նախընտրում են հարձակում գործել միանգամից մի քանի փոքր կազմակերպությունների վրա: Առանձին-առանձին հարձակումներից ստացված շահույթը ավելի քիչ է, բայց եթե այդ կազմակերպությունները բավարար պաշտպանված չեն կամ ընդհանրապես չունեն պաշտպանական համակարգ, ապա կիբեռհանցագործները կտիրանան նրանց գումարներին առանց մեծ ջանքերի: 10-20 փոքր կազմակերպությունների վրա հարձակումից ստացված գումարը կարող է հավասարվել մեկ խոշոր կազմակերպությունից գողացված գումարին:

Քանի որ փոքր կազմակերպությունները ժամանակ չունեն պաշտպանական համակարգ ներդնելու համար, որոշ կիբեռհանցագործներ հարձակման համար նպատակադրված ընտրում են փոքր կազմակերպությունները՝ հուսալով հեշտությամբ ձեռք բերել նրանց գումարները: Թույլ մի տվեք, որ ձեր ընկերությունը լինի դրանց թվում:

Կիբեռհանցագործները օգտագործում են փոքր կազմակերպությունները՝ խոշորները խոցելու համար

Կիբեռհանցագործները գիտեն, որ ոչ մեծ ձեռնարկությունները հաճախ հանդիսանում են մեծերի մատակարարը: Եվս մեկ պատճառ փոքրերի վրա հարձակվելու համար: Հարձակում գործելով փոքր ձեռնարկության վրա կիբեռհանցագործները կարող են ձեռք բերել այնպիսի ինֆորմացիա, որը նրանց հնարավորություն կտա կազմակերպել հարձակում մեծ կորպորացիայի վրա: Հանցագործները նպատակադրված ընտրում են այն փոքր ձեռնարկությունները, որոնք կապված են մեծ կորպորացիաների հետ: Հանցագործները կարող են օգտվել ընձեռված հնարավորությունից և գողանալ փոքր կազմակերպության հաճախորդների տվյալները:

Եթե հանցագործները խոցեն մեծ կազմակերպությունը և հետագայում պարզվի, որ փոքր ձեռնարկությունից գողացած տվյալների միջոցով է իրականացվել հարձակումը, ապա այդ ձեռնարկությանը սպասվում են անախորժություններ:

Եթե անգամ փոքր ձեռնարկությունը հակաօրինական ոչինչ չի արել, պաշտպանական միջոցների բացակայությունը հնարավոր է դարձրել խոցել համակարգը և կազմակերպել հարձակումը մեծ կազմակերպության վրա: Երբ պարզվի փոքր ձեռնարկության դերը հարձակման գործում, նրա դեմ կարող է սկսվել դատական պրոցես, նա ստիպված լինի փոխհատուցում և տուգանք վճարել, կկորցնի հաճախորդներին և իր գործարար վարկանիշը:

Կրկնակի անհաջողություն

Պատկերացնենք փոքր ձեռնարկություն, որը հումքը գնում է մեծ կորպորացիայից, իսկ հետո պատրաստի արտադրանքը վաճառում է միջազգային կազմակերպությանը: Արդյունավետությունը բարձրացնելու նպատակով հումքի մատակարարը օգտագործում է առցանց համակարգեր՝ պատվերների մասին տվյալները մշակելու և հաճախորդների հետ փոխգործակցության համար: Հաճախորդների թվում է նաև այդ փոքր ձեռնարկությունը: Միջազգային կազմակերպությունը պահանջում է, որ ձեռնարկությունը էլեկտրոնային հաշիվները ուղարկի իր հաշվապահական ներքին համակարգերին: Ստացվում է, որ ձեռնարկությունը ուղղակի միանում է մատակարար կազմակերպության և միջազգային կազմակերպության համակարգչային համակարգերին: Եթե կիբեռհանցագործը խոցի ձեռնարկության համակարգիչները՝ նա կստանա այն ինֆորմացիան, որը հնարավոր է դարձնում հարձակումը և մատակարարի, և ձեռնարկության վրա: Եթե այդ հարձակումները հաջողությամբ չավարտվեն, փոքր ձեռնարկությունը ստիպված է լինելու մի շարք հարցերի պատասխանել: Հնարավոր է, որ նա այլևս չկարողանա օգտվել մատակարարների և հաճախորդների էլեկտրոնային համակարգերից: Այս հանգամանքը կանդրադառնա ձեռնարկության աշխատանքի արդյունավետության և շահութաբերության վրա:

Գլուխ 2
ԻՆՉ Է ՊԵՏՔ ՁԵՐ ԿԱԶՄԱԿԵՐՊՈՒԹՅԱՆԸ

Այս գլխում՝

- *Իրավական և նորմատիվ պարտականությունների իմացություն:*
- *Ձեր բնագավառում սպասելիքների գնահատում:*
- *Ինչու սպառնալիքներն այսօր ավելի վտանգավոր են, քան երբևէ:*
- *Անվտանգության նկատմամբ տարբեր պահանջների դրսևորում:*

Այս գլխում մենք կդիտարկենք տարբեր տեսակի կազմակերպությունների համար անվտանգության պահանջների ընդհանրությունները և տարբերությունները:

ԱՆՎՏԱՆԳՈՒԹՅԱՆԸ ՎԵՐԱԲԵՐՈՂ ՄԻ ՔԱՆԻ ՊԱՀԱՆՋՆԵՐ, ՈՐՈՆՔ ՆՈՒՅՆՆ ԵՆ ԲՈԼՈՐ ԸՆԿԵՐՈՒԹՅՈՒՆՆԵՐԻ ՀԱՄԱՐ

Բազմաթիվ ընկերություններ կարծում են, թե իրենք չունեն այն ինֆորմացիան, որը կարող է հետաքրքիր լինել կիբեռհանցագործների համար: Գործարարները գտնում են, որ ինֆորմացիայի կորուստը իրենց ընկերությանը զգալի վնաս չի հասցնի: Ցավոք սրտի այդպես չէ: Սովորական տեղեկատվական բազան՝ հաճախորդների անձնական տվյալներով, արժեքավոր է կիբեռհանցագործների և ձեր մրցակիցների համար:

Ձեր հաճախորդները կարող են դառնալ մրցակիցների հաճախորդները:

Իրավական պարտավորություններ ինֆորմացիայի պաշտպանության համար

Շատ երկրներում ընկերություններին խիստ պահանջներ են դրված անձնական տվյալների օգտագործման աշխատանքում: Եթե չեն կատարվում այդ պահանջները՝ պատժում են խոշոր տուգանքներով, որոշ դեպքերում հայց է ուղղվում ընկերության տնօրենի դեմ, իսկ որոշ խախտումների համար նախատեսված է բանտարկություն:

Որոշ երկրներում անձնական տվյալների օգտագործման և պահպանման համար խոշոր կազմակերպությունների նկատմամբ կիրառում են ավելի խիստ օրենսդրական և նորմատիվ պահանջներ: Եթե տեղի իշխանությունները խոշոր կազմակերպություններից պահանջում են ներդնել անվտանգության ավելի բարդ մեխանիզմներ, ապա փոքր կազմակերպությունները նույնպես պետք է պատասխանատու վերաբերմունք ունենան կարևոր ինֆորմացիայի պաշտպանությունը ապահովելու հարցում:

Այն ընկերությունները, որոնք անտեսում են բիզնեսի և կազմակերպության տվյալ տեսակի համար անվտանգության պարտադիր միջոցառումները, կարող են անախորժությունների հանդիպել:

Ավելի խիստ պահանջներ անվտանգությանը

Մի շարք իրավական նորմեր պարտավորեցնում են ընկերություններին մեծ զգուշավորություն ցուցաբերել գաղտնի նյութերի կամ ինֆորմացիայի հետ աշխատելիս: Ինֆորմացիայի կորուստը երրորդ կողմին կարող է էական վնաս հասցնել:

Շուկայի որոշ ճյուղերի և բաժինների համար ինֆորմացիայի պաշտպանության հարցում կարող են գործել ավելի խիստ պահանջներ: Օրինակ, իրավաբանական և բժշկական ոլորտում աշխատող ընկերությունները պետք է հատուկ զգուշավորություն ցուցաբերեն իրենց մոտ պահվող և օգտագործվող ինֆորմացիայի նկատմամբ:

Եթե անգամ խիստ պահանջները չեն վերաբերում ձեր կազմակերպությանը, գաղտնի ինֆորմացիայի արտահոսքը ձեզ համար կունենա տխուր հետևանքներ:

Վտանգված է անգամ կատուն

Այնպիսի մի ձեռնարկություն, ինչպիսին կատուների և շների համար հյուրանոցն է, բավական հեռու է տեղեկատվական տեխնոլոգիաներից: Կարիք կա՞ մտածել ինֆորմացիոն անվտանգության մասին այս դեպքում: Իհարկե: Հյուրանոցի համակարգչում պահվում են հաճախորդների հասցեները և անունները, կենդանիների ժամանման օրերը: Եթե Բարսիկին կամ Ոեքսին բերել են հյուրանոց, նշանակում է՝ կենդանիների տերերը տանը չեն: Այս տեղեկությունը ստանալով գողերը կարող են հեշտությամբ թալանել այդ տները:

ԸՆԿԱԼՄԱՆ ԵՎ ՌԵՍՈՒՐՍՆԵՐԻ ՏԱՐԲԵՐ ՄԱԿԱՐԴԱԿՆԵՐ

Չնայած ինֆորմացիայի պաշտպանության ստանդարտների որոշ նմանությանը, կա հստակ տարբերություն, թե ինչպես պետք է դիտարկեն և լուծեն տարբեր մեծության ընկերությունները անվտանգության հարցերը:

Այլ ժամանակներ են

Ինֆորմացիոն համակարգերի վրա հարձակումների ժամանակակից կատարելագործված և անխնա բնույթը ցույց է տալիս, որ սպառնալիքները ավելի են մեծացել: Այն ընկերությունները, որոնք այս փաստը չեն գիտակցում, իրենց մեծ ռիսկի են ենթարկում:

Խոշոր ընկերությունները իրենց ինֆորմացիոն համակարգերը պաշտպանելու համար կարող են ունենալ SS անվտանգության մասնագետներ, իսկ ոչ մեծ ձեռնարկությունները չունեն այդ հնարավորությունը:

Արդյո՞ք չափը էական է

Բացահայտ է, որ մատչելի ռեսուրսների ծավալն այն գործոնն է, որով տարբերվում են փոքր ձեռնարկությունները խոշոր կորպորացիաներից: Խոշոր ընկերությունները կարող են հաստիքով վարձել փորձագետների, որոնք որակավորված որոշում կկայացնեն, թե պաշտպանական որ տեխնոլոգիաների համար արժե ներդրում կատարել: Խոշոր ընկերությունները ունեն ֆինանսական անհրաժեշտ միջոցները և օժանդակ ռեսուրսները ընդունած որոշումը իրագործելու համար: Խոշոր ընկերության մասնագետների թիմը անվտանգության պլանների և քաղաքականության մշակման և անընդհատ կատարելագործման

փորձ ունի, ինչը հնարավորություն է տալիս ընկերությանը մեկ քայլ առաջ լինել կիբեռհանցագործներից և պաշտպանական համակարգում չունենալ սողանցքեր:

Փոքր ընկերությունները կարող են այդ հնարավորությունները չունենալ: Աճող ընկերությունը սովորաբար զարգանում է մի քանի ուղղությամբ և այդ ուղղությունները զարգացնելու համար անհրաժեշտ են ֆինանսական միջոցներ: Հետևաբար համակարգչային անվտանգությունը ընկերության առաջնահերթության ցուցակում պետք է ունենա իր տեղը և նրա ներդրումը պետք է արդարացնի ֆինանսական ծախսերը:

ԱՆՎՏԱՆԳՈՒԹՅԱՆԸ ՎԵՐԱԲԵՐՈՂ ՊԱՀԱՆՋՆԵՐԻ ՏԱՐԲԵՐՈՒԹՅՈՒՆՆԵՐԸ

Տարբեր տիպի ընկերությունների ինֆորմացիոն պաշտպանությանը վերաբերող պահանջներն ունեն շատ ընդհանրություններ, բայց կան և տարբերություններ: Ընկերության զարգացման հետ փոխվում են նրա պահանջները ինֆորմացիոն անվտանգության նկատմամբ:

Ձեզ ծանոթ են հետևյալ տիպի ընկերությունները և նրանց վերաբերմունքը SS անվտանգությանը:

Ստարտապ

Սկսնակ գործարար 36 ամյա Տիգրանը լքում է քաղաքի կենտրոնում գտնվող մեծ ընկերությունը և իրավաբան ընկերների հետ հիմնում է նոր ընկերություն:

Ինչպես են օգտագործում SS-ն այդ ընկերությունում.

→ *Տիգրանը և գործընկերները չեն կարող աշխատել առանց նոութբուքների, պլանշետների և սմարթֆոնների, քանի որ դրանցով կարելի է աշխատել ամեն տեղ,*

→ *Ընկերության նորաթուխ տերերը նախատեսել են ինտենսիվ օգտագործել Էլեկտրոնային փոստը հաճախորդների հետ շփման համար, իսկ համակարգիչները՝ նամակների, առաջարկների, նշումների համար:*

Ընկերության վերաբերմունքը անվտանգությանը

→ *Ընկերությունը տիրապետելու է հույժ գաղտնի ինֆորմացիայի՝ այդ թվում ֆինանսական, որի պաշտպանության ապահովումը շատ կարևոր է,*

→ *Ինֆորմացիայի կորուստը կամ արտահոսքը շատ խնդիրներ կստեղծի Տիգրանի և նրա ընկերության համար, կարող է Տիգրանի դեմ դատական գործ հարուցվի,*

→ *Ընկերության ինֆորմացիոն պաշտպանությունը ունի բացառիկ կարևորություն: Տիգրանը գիտակցում է, որ ստանդարտ հակավիրուսային ծրագրային ապահովումը բավարար չէ:*

Տիգրանն ասում է. «Մենք պետք է գնենք և տեղադրենք հակավիրուսային նոր լուծում: Միաժամանակ մենք հնարավորինս արագ պետք է սկսենք եկամուտ ստանալ, այդ պատճառով մեր ընտրած ծրագրային ապահովումը պետք է ապահովի պաշտպանության անհրաժեշտ մակարդակ, լինի պարզ համալարման, կառավարման և սպասարկման համար: Ծրագրային ապահովման մատակարարը պետք է անհրաժեշտության դեպքում մեզ սատարի, որպեսզի մենք կենտրոնանանք հաճախորդների սպասարկման գործին: Պաշտպանական ծրագիրը հեշտությամբ պետք է հարմարվի նոր պահանջներին, որոնք առաջանում են մեր բիզնեսի զարգացման հետ»:

Զարգացող բիզնես

48 տարեկան Հայկը իր բիզնեսում նվաճումներ ունի: Նա տղամարդու հագուստ կարող արհեստանոցների ցանցի սեփականատեր է: Ցանցում աշխատում է 18 մարդ: Հայկի բիզնեսը ընդլայնվում է:

Ինչպես են օգտագործում SS-ն այդ ընկերությունում.

→ *Ընկերությունը բացում է նոր խանութ և դրան զուգահեռ գործարկում է կայքէջ՝ համացանցի միջոցով կոստյումները վաճառելու համար,*

→ *Քանի որ ընկերությունը ընդլայնվում է՝ անհրաժեշտ է ձեռք բերել նոր սարքավորումներ՝ վճարման համար լրացուցիչ սարքեր (PoS), համակարգիչներ, ցանցային Wi-Fi ուղղորդիչներ և նոր սերվեր:*

→ *Չնայած, որ Հայկը մեծ ուշադրություն չի դարձնում SS նորույթներին, նա իր նոր սմարթֆոնը օգտագործում է էլեկտրոնային փոստից օգտվելու համար:*

Ընկերության վերաբերմունքը անվտանգությանը՝

→ *Ընկերությունը օգտվում է հակավիրուսային արտադրանքից, որը համակարգիչների խանութից գնել է Հայկի «տեխնոլոգիաներից հասկացող» զարմիկը: Հայկը հասկանում է, որ բիզնես-ինֆորմացիայի հուսալի պաշտպանության համար այդ արտադրանքը բավարար չէ, մանավանդ ընկերության գործունեության ընդլայնումը հաշվի առնելով: Հայկը չի կարող թույլ տալ, որ իր մրցակիցը ձեռք բերի ընկերության մշտական հաճախորդների ցուցակը և գնացուցակը,*

→ *Հայկը պարտավոր է պահպանել վճարման քարտերի տվյալները պաշտպանելու ստանդարտ պահանջները, դրա համար նա պետք է տեղադրի պաշտպանական ծրագրային ապահովում և պահի դրա բազաները արդիական վիճակում, որպեսզի ապահովի SS անվտանգությունը:*

Հայկն ասում է. «Իմ կյանքի գործը՝ հագուստ կարելն է, այլ ոչ թե ինֆորմացիոն տեխնոլոգիաները: Բայց հիմա պետք է ձեռք բերել անվտանգությունը ապահովող որակավորված լուծում, որպեսզի հետո հանգիստ սրտով նվիրվել սիրելի գործին: Մեզ պետք է մի արտադրանք, որը կապահովի բավարար պաշտպանությունը, որը հեշտ կլինի տեղադրել և կառավարել: Ինձ պետք է ծրագրային այնպիսի ապահովում, որը կկատարի իր գործը և թույլ կտա, որ ես զբաղվեմ իմ գործով: Այն ժամանակից, երբ ես սկսեցի կառավարել հորս բիզնեսը, այն բավական ընդլայնվել է: Հիմա մենք բացում ենք հինգերորդ խանութը և սկսում ենք վաճառքը իրականացնել կայքէջի միջոցով, հետևաբար մեզ անհրաժեշտ է պաշտպանական այնպիսի լուծում, որը կզարգանա մեզ հետ»:

Անվտանգության նկատմամբ մոտեցումը վերանայող կազմակերպություն

Վրդովված քառասունամյա բժշկուհի Անին գլխավորում է բժշկական կաբինետը, որտեղ աշխատում են ևս երկու բժիշկ, մեկ ֆիզիոթերապևտ և երեք ադմինիստրատոր, որոնք աշխատում են կես օր:

Ինչպես են օգտագործվում SS-ն ընկերությունում.

→ *Յուրաքանչյուր բժիշկ ունի իր համակարգիչը, մեկն էլ դրված է ֆիզիոթերապևտի սենյակում: Երկու համակարգիչ կա վիճակագրական բաժնում, մեկը՝ ադմինիստրատորի սենյակում:*

→ *Համացանցը և համակարգիչները փոփոխել են բժշկական այս ընկերության աշխատելաոճը՝ հեշտացել է հիվանդների մասին գրառումներ կատարելը, նոր դեղամիջոցների և պրոցեդուրաների մասին տեղեկություններ ստանալը,*

Ընկերության վերաբերմունքը անվտանգությանը.

→ *Հաշվի առնելով ընկերության կախվածությունը SS-ից և իրենց ունեցած ինֆորմացիայի հույժ գաղտնիությունը, Անին գիտակցում է SS պաշտպանության համար ծրագրային ապահովման անհրաժեշտությունը,*

→ *Այս պահին օգտագործվող ծրագրային ապահովումը նյարդայնացնում է բոլորին՝ համակարգիչները բեռնվում են շատ երկար, իսկ երբ ստուգվում է վնասակար ծրագրերի առկայությունը՝ համակարգիչները «կախում» են:*

Անին ասում է. «Ամենակարևորը հիվանդների մասին ունեցած տվյալների գաղտնիությունն է: Մենք հասկանում ենք պաշտպանական ծրագրային ապահովման անհրաժեշտությունը, այսօր մեր ունեցածը զգալիորեն նվազեցնում է մեր համակարգիչների արտադրողականությունը:

Շուտով լրանում է հավաստագրի ժամկետը, ժամանակն է ձեռք բերել պաշտպանական այլ արտադրանք, որը չի նվազեցնի համակարգիչների արտադրողականությունը և հնարավորություն կտա ավելի արդյունավետ աշխատել հիվանդների հետ: Մեզ պետք է միջոց, որը կպաշտպանի հույժ գաղտնի ինֆորմացիան՝ չխանգարելով հիվանդների որակյալ սպասարկումը»:

Ընկերություն, որն արդեն տուժել է

Երեսուներկու տարեկան Լուսինեն ղեկավարում է մարքետինգի գործակալությունը, որտեղ աշխատում է 22 մարդ: Լուսինեյին հաջողվել է արագ զարգացնել բիզնեսը: Վաճառքի և մարքետինգի ոլորտում իր ունակությունների շնորհիվ նա հեշտությամբ գրավում է նոր հաճախորդների:

Ինչպես են օգտագործում SS-ն ընկերությունում.

→ *Հիմնական աշխատակազմը գտնվում է գրասենյակում, բայց շատերն էլ այցելում են հաճախորդներին,*

→ *Դիզայներների թիմը օգտագործում է «Apple» համակարգիչները, իսկ մյուսները համակցում են համակարգիչը և նոութբուքը կամ համակարգիչը և սմարթֆոնը,*

→ *Աշխատակիցներից շատերը օգտագործում են իրենց անձնական պլանշետները, որոնք ընկերությանը պատկանող սարքեր չեն: Լուսինեն ուրախ է, որ աշխատակիցները օգտագործում են անձնական սարքերը: Նրա կարծիքով, հետևելով այդ նորաձևությանը, իր գործակալությունը շատ ժամանակակից է:*

Ընկերության վերաբերմունքը անվտանգությանը.

→ *Ցավոք, գործակալությունում վերջերս անվտանգության հետ կապված միջադեպ է տեղի ունեցել: Հաճախորդի հետ հանդիպումից հետո աշխատակիցը նոութբուքը վերցրել և գնացել է սրճարան, որտեղից նոութբուքը գողացել են: Նոութբուքում պահվում էին հույժ գաղտնի ֆայլեր, այդ թվում նոր արտադրանքի թողարկման պլաններ, արտադրանք, որը հաճախորդին տվյալ շուկայում կապահովեր առավելություն:*

→ *Լուսինեն պատմել էր եղելությունը հաճախորդին, ինչը նրան զայրացրել էր: Միջադեպով զբաղվում էր հաճախորդի իրավաբանական բաժինը: Հաճախորդը պատրաստվում է խզել կապերը գործակալության հետ, այդ պատճառով նա կկորցնի իր բիզնեսի զգալի մասը: Գործակալության համար կարող են լինել իրավական հետևանքներ:*

Լուսինեն ասում է. «Իմ գլխավոր խնդիրն է բացառել նման միջադեպի կրկնվելը: Մենք պետք է, որքան հնարավոր է արագ, ներդնենք տվյալների պաշտպանության համալիր լուծում: Այն պետք է հեշտությամբ կառավարվի, որպեսզի ես կարողանամ մեր դիզայներներից մեկին, ով գիտակ է տեխնիկական հարցերում, հանձնարարել դրա համալարումը և սպասարկումը»:

Ինքնավստահ ընկերություն

Անհոգ Արամը 53 տարեկան է, նա ունի հաշվապահական ընկերություն, որտեղ աշխատում է հինգ մարդ: Կայացած ընկերությունը անվտանգությանը վերաբերող վտանգներին լուրջ չի վերաբերվել: Արամի դիրքորոշումն էր՝ ինձ ոչ մի վատ բան չի պատահի:

Ինչպես են օգտագործում SS-ն ընկերությունում

→ *Արամը և հաշվապահական հարցերով երկու խորհրդատուները շատ ժամանակ են անցկացնում հաճախորդների հետ: Նոութբուքերի առկայությունը հնարավորություն է տալիս անընդհատ չլինել գրասենյակում:*

→ *Ընկերության երկու ադմինիստրատորները օգտագործում են համակարգիչներ,*

→ *Ընկերությունը օգտագործում է ֆայլային սերվեր, որի վրա տեղադրված է CRM (Հաճախորդների հետ հարաբերությունների կառավարում) համակարգը:*

Ընկերության վերաբերմունքը անվտանգությանը.

→ *Տնտեսագիտական մի ամսագրում Արամը կարդացել է, որ մրցակից ընկերությունը տուժել է ինֆորմացիոն անվտանգության համակարգում առկա սողանցքի պատճառով: Ադմինիստրատորը ներբեռնել է վնասատու ծրագրով ֆայլը, որը եղել է էլեկտրոնային նամակի մեջ: Վնասատու ծրագիրը թափանցել է հաճախորդների գաղտնի ֆայլերի մեջ: Խնդիրը բացահայտվել է այն ժամանակ, երբ հաճախորդներից մեկը տեսել է, որ իր գաղտնի տվյալները վաճառվում են համացանցում,*

→ *Հոդվածը կարդալուց հետո Արամը անհանգստացել է սեփական ընկերության SS անվտանգության համար: Նա հասկանում է, որ իրենց օգտագործած անվճար լուծումը հավանական է, որ չի ապահովում անվտանգության անհրաժեշտ մակարդակը:*

Արամը ասում է. «Վերջին տարիներին, այն ոլորտը, որում մենք աշխատում ենք, փոխվել է: Այժմ կան օրենսդրական մի շարք պահանջներ: Առկա վտանգների բնույթը ստիպում է ներդնել ավելի ապահով SS պաշտպանություն»:

Տարբեր լուծումներ տարբեր պահանջմունքների համար

Այս գլխում դիտարկված ընկերությունները գործում են տարբեր շուկաներում և տարբեր ձևով են օգտագործում SS-ները: Նրանք ունեն մի ընդհանրություն՝ պաշտպանել արժեքավոր ինֆորմացիան: Ընկերությունները օգտագործում են տարբեր սարքավորումներ և SS ոլորտում տարբեր են նրանց որակավորումները, հետևաբար պաշտպանության տարբեր տեսակներ են նրանց անհրաժեշտ:

Իհարկե, մեր բերած օրինակները ընդհանրացված են՝ ամեն մի ձեռնարկություն իր վերաբերմունքն ու պահանջներն ունի SS անվտանգության նկատմամբ: Բիզնես-մոդելները և ընկերությունների տեսակները անթիվ են և նրանց պահանջները SS նկատմամբ պայմանավորված են գործունեության տեսակով:

3-5 մարդուց բաղկացած ընկերությունը կարող է համակարգիչների միջոցով ղեկավարել խոշորամասշտաբ գործընթացներ: Նման ընկերությունը պետք է որ ունենա բազմապլան SS ենթակառուցվածք և նրան անհրաժեշտ է պաշտպանական այնպիսի լուծում, որը հաշվի կառնի ընկերության SS միջավայրի բոլոր դժվարությունները:

Գլուխ 3

ՈՂՋ ՃՇՄԱՐՏՈՒԹՅՈՒՆԸ ԱՆՎՏԱՆԳՈՒԹՅԱՆԸ ՍՊԱՌՆԱՑՈՂ ՎՏԱՆԳՆԵՐԻ ՄԱՍԻՆ

Այս գլխում՝

- *Բարդ SS-երը ավելացնում են նոր խնդիրներ:*
- *Ինչու՞ միայն հակավիրուսային պաշտպանությունը բավարար չէ:*
- *Ծանոթություն ինտերնետ-վտանգների հետ:*
- *Ինտերնետ-բանկինգի տրանզակցիաների պաշտպանությունը:*

Այս գլխում մենք կդիտարկենք, թե ինչպես բիզնեսի համար տիպային ծրագրային լուծումների բարդացումը և համակարգչային վիրուսների, վնասատու ծրագրերի և կիբեռհարձակումների կատարելագործումը դժվարեցնում են ընկերությունների գործունեությունը:

ԱՄԵՆ ԻՆՉ ԲԱՐԴԱՑԵԼ Է

Դեռևս մի քանի տարի առաջ բոլոր սարքավորումները, որոնք պաշտպանության կարիք ունեին, գտնվում էին ընկերության ղեկավարի «տեսանելիության դաշտում»: Կարելի էր բոլոր համակարգիչների մեջ տեղադրել անհրաժեշտ ծրագրային ապահովումը և պաշտպանված համարվել: Այդպես էր այն ժամանակ, երբ բիզնես-ինֆորմացիան գրասենյակից դուրս հասանելի չէր:

Ընկերությունները չեն կարող գործել առանց SS-ի

Իհարկե դուք չեք կարող ղեկավարել ձեր ընկերությունը չօգտագործելով բիզնես-հավելվածը և բիզնես- ինֆորմացիայի հասանելիությունը ապահովող բջջային սարքավորումները: Տեխնոլոգիական այդ նվաճումները բերում են որոշակի հեռևանքների: Կորպորատիվ ռեսուրսներին հեռվից հասանելի լինելու հնարավորությունը ավելի է բարդացնում SS-ները: Եթե դուք և ձեր աշխատակիցները ուզում եք, որ ինֆորմացիան հասանելի լինի նոութբուքների, սմարթֆոնների և պլանշետների միջոցով, ապա որտեղ է այն սահմանագիծը, որի ներսում ձեր ընկերությունը պաշտպանված է:

BYOD-ը բարդության ևս մեկ աստիճան է ավելացնում

Ամեն ինչ ավելի է բարդանում, երբ օգտագործվում է BYOD-ը (Bring Your Own Device - աշխատակիցները օգտագործում են սեփական սարքավորումները)՝ աշխատակիցների համար ընկերության համակարգերը և ինֆորմացիան հասանելի են սեփական սարքավորումների միջոցով: Աշխարհի ցանկացած կետից ցանկացած սարքավորման միջոցով հասանելիությունը պաշտպանական համակարգի համար խնդիրներ է առաջացնում:

Ընկերությունները արագ գնահատեցին BYOD-ի պոտենցիալ առավելությունները միջոցների տնտեսման և արտադրողականության բարձրացման տեսանկյունից: BYOD օգտագործելիս նշանակում է ապահովել ընկերությանը պատկանող և չպատկանող բջջային տարբեր սարքերի՝ այդ թվում Android, iPhone, BlackBerry, Symbian, Windows Mobile, Widows Phone տարբեր մոդելների անվտանգությունը:

Բարեբախտաբար, անվտանգությունը ապահովող արտադրանք մատակարարողները արագ հասկացան, որ SS բարդացումը փոքր ձեռնարկությունների տերերի համար գլխացավանք է: Այդ պատճառով նրանք ստեղծեցին նորարարական լուծումներ, որոնք ավելի են պարզեցնում տարբեր սարքավորումների պաշտպանությունը:

Վիրուս, թե վնասատու ծրագրային ապահովում

Որոշ ընկերություններ կարծում են, թե վիրուսը և վնասատու ծրագրային ապահովումը նույն բանն են և դրանց դեմ պայքարելու համար միջոցները նույնն են: Իհարկե այդպես չէ, նման մոտեցումը շատ թանկ կնստի ընկերության վրա: Շատերը ծանոթ են համակարգչային վիրուսներին, որոնք անցնում են մի համակարգից մյուսը: «Վնասատու ծրագրային ապահովում» հասկացությունը ընդգրկում է վտանգավոր ծրագրերի մեծ խումբ: Բացի համակարգչային վիրուսներից դրա մեջ մտնում են որդերը, տրոյացիները, ստեղնաշարային լրտեսները, լրտեսական ծրագրային ապահովումը, կորզիչ-ծրագրերը և այլ վտանգներ:

Վնասատու ծրագրային ապահովումից պաշտպանող ծրագրային արտադրանքը պաշտպանում է ինֆորմացիան և համակարգիչները ոչ միայն վիրուսներից, այլ ավելի մեծ վտանգներից:

ՎՏԱՆԳՆԵՐԻ ՍՊԱՌՆԱԼԻՔԸ ԱՆՇԵՂՈՐԵՆ ԱՃՈՒՄ Է

Բոլոր օգտատերերը այս կամ այն չափ գիտեն, թե ինչ բան է համակարգչային վիրուսը: Քիչ են այն մարդիկ, որոնց համակարգչում չի հայտնվել վիրուս: Անցել է այն ժամանակը, երբ կիբեռխուլիգանները վիրուսները ստեղծում էին զվարճանքի համար: Այսօր վնասատու ծրագրային ապահովման կիրառության նպատակն է ֆինանսական շահույթ ստանալը:

Անմեղ կատակների ժամանակն անցել է

Նախկինում կիբեռխուլիգանությունը ուսանողների և դպրոցականների գործն էր: Նրանք այդպիսով ցանկանում էին ցույց տալ իրենց ունակությունները: Նրանք ստեղծում և տարածում էին վիրուսներ, որոնք այս կամ այն կերպ խափանում էին վարակված համակարգչի աշխատանքը, օրինակ՝ հեռացնում էին մի քանի ֆայլ կամ «կախում» էին համակարգիչը: Չնայած, որ այսպիսի ծրագրերը որոշ անհարմարություններ էին ստեղծում, համարվում էին անմեղ զվարճանք:

Վիրուսներն ընկերությունների համար հազվադեպ էին խնդիրներ առաջացնում և մարդկանց ու կազմակերպությունների բանկային հաշիվներից գումար չէին գողանում: Բացի այդ, հենքային հակավիրուսային ծրագրային ապահովումը հեշտությամբ պաշտպանում էր հարձակումներից:

Խուլիգանությունից հանցագործություն

Վերջին տարիներին երիտասարդ համակարգչային գիկերը (մարդիկ, ովքեր հմտացած են բարձր տեխնոլոգիաների բնագավառում) նախընտրում են իրենց վարպետությունը ցուցադրել առցանց խաղերում:

Համացանցի միջոցով կատարվող բիզնես-գործընթացների և ֆինանսական գործողությունների ծավալի աճը էապես մեծացրել է մեր կախվածությունը համացանցից և էլեկտրոնային առևտրից:

Անմեղ կիբեռխուլիգանությունների ժամանակը անցել է, համացանցը ավելի լուրջ վտանգներով է սպառնում:

Կիբեռհանցագործները արագ հասկացան, որ վնասատու ծրագրային ապահովումը և ինտերնետ-խարդախության այլ գործիքներ կարելի է օգտագործել ավելի լուրջ նպատակների համար, քան կատակը և խուլիգանությունը: Ժամանակակից հարձակումները մշակվում են ինֆորմացիայի, փողի և այլ արժեքներ գողանալու համար: Կիբեռհանցագործները, ովքեր ունեն տեխնիկական ազդեցիկ հմտություններ, անընդհատ մշակում են նորանոր մեթոդներ՝ ընկերությունների վրա հարձակվելու համար: Հիմնականում այդ արվում է ֆինանսական շահույթի համար՝ ընկերությունների բանկային հաշիվներից գողանում են գումարներ, գողանում են գաղտնիք հանդիսացող բիզնես-տվյալներ, որոնք հետո կարելի է վաճառել «սև» շուկայում, ընկերության անունից անօրինական վճարումներ են կատարում:

Ընկերության նոութբուքերից, սերվերներից և բջջային սարքերից քաղած ինֆորմացիան հնարավորություն է տալիս կիբեռհանցագործներին գողանալ այն ֆիզիկական անձանց փողերը, ովքեր կապված են ընկերության հետ:

Համակարգիչներից կախվածությունը հեշտացրել է բիզնես-համակարգերի աշխատանքի խախտումը սոցիալական կամ քաղաքական բողոք արտահայտելու համար:

ԻՄԱՑԻՐ ՔՈ ԹՇՆԱՄՈՒՆ ԵՎ ՆՐԱ ՄԵԹՈԴՆԵՐԸ

Վնասատու ծրագրային ապահովումը և SS անվտանգության սպառնալիքները ընկերություններին կարող են մեծ վնաս հասցնել, իսկ ոչ մեծ ձեռնարկությունների համար կարող են կործանարար լինել: Այս գլխում ներկայացված են ոչ բոլոր վտանգները, բայց դրանք էլ պատկերացում են տալիս անվտանգության այն ռիսկերի մասին, որոնց պետք է պատրաստ լինեն ընկերությունները:

Վիրուսներ, որդեր, տրոյացիներ

Համակարգչային վիրուսները և որդերը վնասատու ծրագրեր են, որոնք կարող են ինքնագործարկվել համակարգիչներում, որոնց տերերը տեղյակ չեն վարակման մասին: Տրոյացիները կատարում են վնասատու գործողություններ, որոնք օգտատերը չի հրահանգել: Տրոյացիները չեն ինքնագործարկվում, բայց համացանցի շնորհիվ կիբեռհանցագործները հեշտությամբ տարածում են դրանք:

Եթե վնասատու ծրագիրը գրոհում է ձեր ցանցը, այն կարող է ջնջել կամ փոփոխել տվյալները, անհասանելի դարձնել դրանք, ընդհատել համակարգիչների աշխատանքը կամ գողանալ գաղտնի տեղեկություն:

Բեկդորներ

Բեկդորները հնարավոր են դարձնում վարակված համակարգիչների հեռահար կառավարումը: Սովորաբար խոցված համակարգիչները դառնում են վնասատու ցանցի մասը, որոնք կոչվում են «բոտ-ցանց», կարող են օգտագործվել հանցագործություն կատարելու համար:

Ստեղնաշարային լրտեսներ

Սա վնասատու ծրագիր է, որը արձանագրում է յուրաքանչյուր ստեղնի սեղմումը: Այսպիսի ծրագրերը օգտագործում են գաղտնի տվյալներ՝ գաղտնաբառերի, բանկային հաշվեհամարների և դրանց կոդերի, կրեդիտ քարտերի ծածկագրերը կորզելու համար:

Սպամ

Սպամի ամենաանմեղ տարբերակը՝ էլեկտրոնային փոստի անցանկալի հաղորդագրություններն են: Սպամը կարող է լինել վտանգավոր, երբ կիրառվում է ֆիշինգ պատերազմներում կամ եթե պարունակում է հղում վարակված կայքէջերին, որոնք ներբեռնում են վիրուսները, որդերը և տրոյական ծրագրերը զոհի համակարգչի մեջ:

Ֆիշինգ

Ֆիշինգը հարձակման բարդ ձև է: Հանցագործները ստեղծում են օրինական կայքի կեղծ տարբերակը, օրինակ՝ ինտերնետ-բանկինգի կամ սոցիալական ցանցի, և երբ օգտատերը այցելում է կեղծ կայք՝ նրանք սոցիալական ինժեներիայի մեթոդներով տիրանում են նրա արժեքավոր ինֆորմացիային:

Ֆիշինգը հաճախ օգտագործում են անձնական տվյալները գողանալու և դրանց միջոցով բանկային հաշիվներից և կրեդիտ-քարտերից փող գողանալու համար:

Կորզող ծրագրեր

Տրոյական կորզող ծրագրերը նախատեսված են փող կորզելու համար: Սովորաբար այդպիսի տրոյական ծրագիրը կամ ծածկագրում է զոհի տվյալները նրա համակարգչի կոշտ սկա-

վառակի վրա, կամ համակարգիչը դարձնում է անհասանելի: Դրանից հետո կորզիչ ծրագիրը այդ փոփոխությունները վերացնելու համար գումար է պահանջում:

Այդպիսի ծրագրերը փոխանցվում են էլեկտրոնային փոստի ֆիշինգ հաղորդագրությունների միջոցով կամ վնասատու ծրագրային ապահովում ունեցող կայքէջ այցելելուց հետո: Վնասատու ծրագրերով կարող են վարակված լինել ամենասովորական կայքէջերը, կորզող ծրագրից կարելի է տուժել ոչ միայն կասկածելի կայքերում:

DDoS-հարձակում

Զեռնարկության համակարգիչները կամ ցանցը հնարավոր չէ ըստ նպատակի օգտագործել, եթե կիրառվել է DDoS հարձակում: Այսպիսի հարձակման հիմնական նպատակը՝ ընկերության կայքէջը շարքից հանելն է:

Ընկերությունները կայքէջերի միջոցով հաճախորդներ են ձեռք բերում և գործակցում են նրանց հետ: Կայքէջի ոչ ճիշտ կամ դանդաղ աշխատանքը, նրա անհասանելի լինելը բիզնեսին զգալի վնաս կարող են հասցնել:

DDoS հարձակումները տարբեր ձևեր կարող են ունենալ: Օրինակ, կիբեռհանցագործները կարող են վարակել մեծ թվով համակարգիչներ, որոնց տերերը տեղյակ էլ չեն այդ մասին, և այդ համակարգիչների միջոցով ընկերության կայքէջին ուղարկում է ոչ պիտանի տվյալների մեծ հոսք: Արդյունքում սերվերը, որի վրա զոհի կայքէջն է, գերբեռնվում է՝ դանդաղեցնելով կայքէջի աշխատանքը կամ լրիվ խափանում:

Ինչպիսի սխալներից է տուժում ընկերությունը

Յուրաքանչյուր ծրագիր և օպերացիոն համակարգ, որն օգտագործում է ձեր ընկերությունը, պարունակում է սխալներ: Սովորաբար այդ սխալները ծրագրային կոդին ուղղակի վնաս չեն տալիս: Բայց դրանցից որոշները առաջացնում են խոցելի տեղեր, որոնք կարող են օգտագործել կիբեռհանցագործները անօրինական ձևով ձեր համակարգիչների մեջ մուտք գործելու համար:

Նման խոցելի տեղերը թույլ են տալիս հանցագործներին թափանցել ընկերության համակարգչային ցանց: Հարձակման այս ձևը շատ տարածված է, այդ պատճառով պետք է տեղադրել հավելվածների անվտանգության նորացումներ և ուղղումներ (մի անտեսեք ծրագրային ապահովման նորացման մասին հիշեցումը):

Անվտանգության ապահովման որոշ լուծումներ ունեն ֆունկցիաներ, որոնք բացահայտում և փակում են ընկերության ցանցում տեղադրված հավելվածների և օպերացիոն համակարգերի խոցելի տեղերը:

ԱՆՎՏԱՆԳՈՒԹՅԱՆ ԱՅԼ ՌԻՍԿԵՐ

Նախորդ բաժնում ներկայացված հարձակումներից բացի ձեր ընկերությունը պետք է զգուշանա և այլ վտանգներից:

Ռիսկերը հանրամատչելի Wi-Fi ցանցերի օգտագործման դեպքում

Այսօր հյուրանոցները, օդանավակայանները և ռեստորանները հաճախորդներին թույլ են տալիս անվճար օգտվել Wi-Fi ցանցերից, և շատերը տեղում ստուգում են իրենց Էլեկտրո-

նային փոստը: Կիբեռհանցագործները նույնպես օգտվում են այս հանգամանքից՝ նրանք հետևում են Wi-Fi հանրամատչելի ցանցերին և կարող են ձեռք բերել այն ինֆորմացիան, որը դուք ուղարկում կամ ստանում եք: Նշանակում է՝ կիբեռհանցագործների համար հասանելի են ձեր կորպորատիվ փոստարկղերը և համակարգչային ցանցը, ինչպես նաև ֆինանսական գործարքների համար օգտագործվող գաղտնաբառերը:

Ինտերնետ-բանկինգը և լրացուցիչ պաշտպանության անհրաժեշտությունը

Ինտերնետ-բանկինգը շատ ընկերությունների համար դարձել է անփոխարինելի գործիք: Այն շատ հարմար է և տնտեսում է ժամանակը: Բայց ֆինանսական ինտերնետ-օպերացիաներ կատարելիս դուք վտանգված եք:

Կիբեռհանցագործները հետևում են զոհի համակարգիչներին և բջջային սարքերին, որպեսզի պարզեն, թե երբ է օգտատերը այցելում բանկի կայքէջ կամ ինտերնետ-վճարման սպասարկում: Հատուկ ծրագիր՝ «ստեղնաշարային լրտեսներ» օգտագործելով իմանում են այն ինֆորմացիան, որը դուք ներմուծեցիք: Նշանակում է, որ կիբեռհանցագործը աննկատ կարող է գողանալ ձեր գաղտնաբառը և ձեր հաշվից գումարը փոխանցել իր հաշվին, իսկ դուք այդ մասին տեղյակ չեք լինի:

Բարեբախտաբար, որոշ պաշտպանական ծրագրային արտադրանքներ ներառում են տեխնոլոգիաներ, որոնք ապահովում են պաշտպանության լրացուցիչ աստիճան, երբ դուք համացանցում ֆինանսական գործարքներ եք կատարում:

Նպատակային ֆիշինգ-հարձակումներ

Նպատակային ֆիշինգ-հարձակումը գրոհի բարդ ձև է: Կիբեռհանցագործները ձգտում են ստանալ օգտատերերի անձնական տեղեկատվությունը՝ լրտեսելով հանրամատչելի Wi-Fi ցանցերը: Օգտագործելով Wi-Fi ցանցերը ստեղծում են էլեկտրոնային փոստի ճշմարտանման («ֆիշինգային») հաղորդագրություն, որի միջոցով փորձում են վնասել ընկերության անվտանգության համակարգը:

Կիբեռհանցագործը սոցիալական ցանցում կարող է կարդալ ձեր աշխատակցի գրառումը անցկացրած արձակուրդի մասին և հետո այդ ինֆորմացիան օգտագործել ֆիշինգային հաղորդագրության մեջ: Երբ մի աշխատակիցը մյուսից ստանում է հաղորդագրություն արձակուրդի մասին, նա հավատում է դրա ճշմարտացիությանը: Եթե հաղորդագրության մեջ գրված լինի հղումով անցնել և հաստատել կորպորատիվ ցանցի հասանելիությունը, ապա կիբեռհանցագործը կկարողանա ստանալ մուտքի գաղտնաբառը:

Կորսված նոութբուքեր

Մենք բոլորս էլ լսել ենք տաքսիներում, գնացքներում, ռեստորաններում մոռացված նոութբուքերի մասին: Հանցագործների ձեռքում գաղտնի ինֆորմացիայի հայտնվելու հավանականությունը սարսափեցնում է: Սովորական անուշադրությունը կարող է մեծ հարված հասցնել ընկերության գործարար վարկանիշին և խոշոր տույժերի պատճառ լինել:

Մասամբ այդ խնդիրը լուծվում է անվտանգության լուծումով, որը ծածկագրում է բիզնես-ինֆորմացիան: Այսպիսով, եթե նոութբուքը կորի կամ գողանան, կիբեռհանցագործների համար հասանելի չեն լինի կոշտ սկավառակի վրա պահվող տվյալները:

Ինչ բան է ծածկագրումը

Ծածկագրումը պաշտպանության ձև է, որը հնարավորություն է տալիս հաղթել կիբեռհանցագործին հենց իր խաղում: Դուք տեսել եք ֆիլմերում, որ լրտեսները այնպես են ծածկագրում հաղորդագրությունները, որ դրանք կարող են կարդալ միայն ծածկագրի բանալին իմացողները: Ծածկագրումը թույլ է տալիս գաղտնագրել ընկերության կարևոր ինֆորմացիան, որը կարելի է գաղտնազերծել հատուկ ծածկագրի միջոցով:

Եթե չարագործները տիրանան ընկերության գաղտնի ինչ-որ տվյալների, նրանք չեն կարող կարդալ այդ նյութը առանց հատուկ բանալու:

Եթե ընկերության տվյալները ծածկագրված են, ապա նոութբուքը կամ կրիչը կորցնելու դեպքում կարող եք չանհանգստանալ գաղտնի բիզնես-ինֆորմացիայի արտահոսքի համար:

Բջջային սպառնալիքներ

Մի շարք օգտատերեր և ընկերություններ սխալմամբ կարծում են, թե սմարթֆոնը կամ iPhone-ը սոսկ հեռախոսներ են: Նման սարքերը հզոր համակարգիչներ են, որոնք կարող են պահել գաղտնի ինֆորմացիայի մեծ ծավալ: Բջջային սարքի կորուստը կամ դրա գողանալը կարող է հանգեցնել անվտանգության լուրջ խնդիրների: Եթե գողացված կամ կորսված սմարթֆոնը չունի պաշտպանող PIN-կոդ (ցանկալի է երկար և բարդ գաղտնաբառ), ցանկացած մեկը կարող է կարդալ այնտեղ արված գրառումները:

Անվտանգությունը ապահովող որոշ լուծումներ ունեն հեռավար ղեկավարման հնարավորություն, որով կարելի է միանալ

կորցրած կամ գողացված հեռախոսին և ջնջել բոլոր տվյալները:

Եթե ձեր ընտրած պաշտպանական լուծումը ունի տվյալների ծածկագրման հնարավորություն, ապա դուք ստանում եք պաշտպանության լրացուցիչ աստիճան: Անգամ եթե հանցագործը գտնի ձեր կորցրած հեռախոսը, ծածկագրումը թույլ չի տա, որ ձեր գաղտնի տվյալները կարդան:

Քանի որ ժամանակակից սմարթֆոնները և պլանշետներն ըստ Էության համակարգիչներ են, դրանք սովորական նոութբուքերի և համակարգիչների պես ենթակա են ցանցահեների հարձակմանը, վնասատու ծրագրային ապահովմամբ վարակվելուն, ֆիշինգին: Այդ պատճառով անհրաժեշտ է բջջային սարքերը պաշտպանել հատուկ ծրագրային ապահովմամբ:

Գլուխ 4

ԻՆՖՈՐՄԱՑԻՈՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ՄԱԿԱՐԴԱԿԻ ԲԱՐՁՐԱՑՄԱՆ ՊԼԱՆԱՎՈՐՈՒՄԸ

Այս գլխում՝

- *Բիզնես-ռիսկերի գնահատման օգտակարությունը:*
- *Անվտանգության ռիսկերի մասին աշխատակիցների տեղեկացված լինելը:*
- *Ինչպես կարող են ամպի տեխնոլոգիաները ազդել անվտանգության վրա:*
- *Ամպի ծառայություններ մատակարարողների գնահատումը:*

Երբ գործը հասնում է SS անվտանգությանը՝ ոմանք մտածում են. «Շատ բարդ գործ է: Հույս ունեմ, որ ինձ այդ պետք չէ»: Հաջողություն մաղթենք այդ մարդկանց: Բայց երբ հաճախորդները կամ բիզնես-գործընկերները տվյալների կորստի դեպքում ընկերության դեմ դատական հայց են ներկայացնում, ընկերությունը չի կարողանում արդարանալ: Այս գլխում կդիտարկենք պաշտպանական մի քանի պարզ միջոցառումներ, որոնք ծախսատար չեն: Կխոսենք նաև այն մասին, թե ինչպես ամպի տեխնոլոգիաները կարող են ազդել ընկերության պաշտպանության ռազմավարության վրա:

ՎՏԱՆԳԱՎՈՐ ԲԻԶՆԵՍ

Շատերին թվում է, թե ռիսկի գնահատումը դժվար խնդիր է, և այն սպիտակ խալաթով և ակնոցով «խելոքների» գործն է: Եթե դուք ուզում եք բարձրացնել ինֆորմացիոն անվտանգության մակարդակը, մենք կկիսվենք ձեզ հետ մի քանի գաղափարով, որոնցով կարելի է ղեկավարվել ձեր բիզնեսի ռիսկերը գնահատելիս:

Սկզբում ձեզ տվեք հետևյալ հարցերը՝

- → *որտե՞ղ է պահվում մեր բիզնես-ինֆորմացիան,*
- → *որքանո՞վ է այն արժեքավոր ընկերության և հնարավոր գողի համար:*
  - ↘ *Եթե գաղտնի ինֆորմացիան ընկնի հանցագործների ձեռքը՝ ի՞նչ հետևանքներ կունենա դա ընկերության համար*
  - ↘ *Ինչպե՞ս կանդրադառնա ինֆորմացիայի արտահոսքը ընկերության հաճախորդների, աշխատակիցների և բիզնես–գործընկերների հետ հարաբերությունների վրա*
  - ↘ *Որքանո՞վ կտուժի ձեր գործարար վարկանիշը*
- → *Ի՞նչ միջոցներ է ձեռնարկում ընկերությունը գաղտնի ինֆորմացիան պաշտպանելու համար*
- → *Արդյո՞ք բավարար են իմ բիզնես-ինֆորմացիայի պաշտպանության միջոցները*
  - ↘ *Որքանո՞վ են ձեռնարկվող միջոցառումները համապատասխանում իմ ոլորտում և այս մեծության ընկերության համար ընդունված նորմերին (բիզնեսի*

ընդլայնման հետ ստիպված եք լինելու ինֆորմացիայի պաշտպանության մակարդակը բարձրացնելու համար միջոցներ ծախսել):

- *Կհամաձայնվի՞ դատարանը, որ իմ ընկերությունը կիրառում է պաշտպանության անհրաժեշտ միջոցառումները:*

→ *Որքանո՞վ է հավանական, որ իմ ընկերությունը կտուժի գաղտնի ինֆորմացիայի արտահոսքից:*

Այս հարցերին պատասխանելով դուք կորոշեք, թե ձեր ընկերության ինֆորմացիոն անվտանգությունը որ ուղղությամբ լավացնել:

ԱՇԽԱՏԱԿԻՑՆԵՐԸ ՍՈՎՈՐՈՒՄ ԵՆ SS ԱՆՎՏԱՆԳՈՒԹՅԱՆ ՀՆԱՐՔՆԵՐԸ

Երբ խոսվում է արժեքավոր ինֆորմացիայի պաշտպանության մասին՝ գործում է «տեղեկացված ես՝ ուրեմն զինված ես» կանոնը: Այդ պատճառով շատ կարևոր է, որպեսզի դուք և ձեր աշխատակիցները պատրաստ լինեք անվտանգության հնարավոր բոլոր ռիսկերին և իմանաք ինչպես խուսափել դրանցից: Զարմանալի է, որ շատ ընկերություններ անտեսում են իրենց աշխատակիցներին անվտանգության տարրական կանոնների ուսուցումը: Հնարավոր ռիսկերի և դրանց դեմ պայքարի մեթոդների մասին մարդկանց պատմելը կիբեռհանցագործներին դիմակայելու ամենապարզ և էժան միջոցն է:

Ընկերության անվտանգության գործում աշխատակիցներին ձեր կողմը գրավելը դժվար չէ:

→ *Դիտարկեք ձեր ընկերությանը սպառնացող բոլոր*

այն ռիսկերը, որոնք բխում են վնասատու ծրագրային ապահովումներից և կիբեռհանցագործություններից, և որոշեք թե ձեր աշխատակիցները ինչպես կարող են օգնել ձեզ խուսափել այդ ռիսկերից: Չնայած, որ ժամանակակից վտանգները հնարամիտ կառուցվածք ունեն, հարձակումների մեծ մասը սկսվում է այն բանից, որ աշխատակցին հրահանգվում է կատարել մի պարզ գործողություն, որը վտանգում է ընկերության անվտանգությունը, օրինակ՝ սեղմել ֆիշինգային հաղորդագրության հղումը:

→ *Մշակեք SS անվտանգության քաղաքականությունը և տվեք ձեր աշխատակիցներին: SS անվտանգության քաղաքականության մեջ պետք է հստակ ձևակերպված լինեն նրանց գործողությունները ռիսկերը կանխարգելելու և անվտանգությունը ապահովելու համար:*

→ *Հաճախակի կազմակերպեք բացատրական ժողովներ, գրավեք աշխատակիցների ուշադրությունը հետևյալ հարցերին՝*

- ↘ *տարբեր հավելվածների և գրանցման հաշիվների համար օգտագործել տարբեր գաղտնաբառեր,*
- ↘ *հանրամատչելի Wi-Fi ցանցերի օգտագործման ռիսկերը և դրանց կանխարգելման միջոցները,*
- ↘ *նպատակային ֆիշինգային հարձակումների բացահայտումը,*
- ↘ *ինչպես կանդրադառնա բջջային սարքի կորուստը ընկերության անվտանգության վրա:*

- → *Ապահովեք անվտանգության քաղաքականության իրագործումը, օրինակ՝ ձեռնարկեք միջոցներ, որպեսզի երաշխավորվի հուսալի գաղտնաբառերի օգտագործումը բիզնես-ինֆորմացիայի, բանկային հաշիվների հասանելիության պաշտպանության համար:*
- → *Աշխատանքային նոր գործընթացների ներդրման և նոր ռիսկերի ի հայտ գալու դեպքում վերանայեք անվտանգության քաղաքականությունը:*
- → *Հաճախակի անցկացրեք ուսուցանող դասընթացներ, որպեսզի աշխատակիցները վերհիշեն SS անվտանգության կանոնները:*
- → *Նոր աշխատակիցների հետ բացատրական աշխատանք տարեք՝ գործին ծանոթացնելիս:*

Որ գաղտնաբառը կարելի է համարել հուսալի

Եթե գաղտնաբառի հիմքում հեշտ հիշվող բառ է կամ թվերի պարզ հաջորդականություն, ապա կիբեռհանցագործը հեշտությամբ կկռահի այն: Հուսալի գաղտնաբառը պետք է կազմված լինի մեծատառերից և փոքրատառերից, թվերից և հատուկ նշաններից, ամբողջը ութ նիշից ոչ պակաս:

Չի կարելի օգտագործել նույն գաղտնաբառը մի քանի հավելվածի կամ գրանցման հաշիվների համար: Եթե կիբեռհանցագործը իմանա աշխատակցի գաղտնաբառը «Facebook»-ի գրանցման հաշվի համար, անթույլատրելի է, որ դրա միջոցով հասանելի լինի կորպորատիվ էլեկտրոնային փոստը:

ԱՄՊԵՐՈՒՄ

Վերջին տարիներին շատ է խոսվում ամպի տեխնոլոգիաների մասին: Տարբեր տեսակի և մեծության ընկերություններ գնահատում են, թե ամպը որքանով է հեշտացնում ինֆորմացիայի պահպանումը և կրճատում ծախսերը:

Երբեմն ոչ մեծ կազմակերպությունները ավելի արագ են փոխառնում նոր բիզնես-ռազմավարությունը, քան խոշորները: Միաժամանակ ոչ մեծ ընկերությունները ավելի սևեռված են իրենց հիմնական գործունեությանը և բավարար ժամանակ չունեն SS անվտանգության խնդրով զբաղվելու համար: Այդ պատճառով ընկերության բուն գործունեությանը չվերաբերող հարցերի լուծումը հանձնարարվում է հրավիրված մասնագետներին:

Ամպի մեջ, թե այլուր՝ ձեր ինֆորմացիայի պահպանված լինելը ձեր խնդիրն է

Եթե դուք ուզում եք բիզնես-ինֆորմացիայի մի մասը կամ ինչ-որ հավելված տեղափոխել ամպի մեջ՝ հիշեք, որ դրանց անվտանգության համար շարունակում է պատասխանատվություն կրել ձեր ընկերությունը: Բացի այդ ամպի մեջ պահելը չի նշանակում, որ ձեր բիզնես-ինֆորմացիան ամբողջությամբ պաշտպանված է: Անկախ այն բանից, թե որտեղ է պահվում ինֆորմացիան, այն պատկանում է ձեր ընկերությանը և այն պաշտպանելու պատասխանատվությունը կրում է ձեր ընկերությունը՝ այդպիսին է օրենքի պահանջը:

Մտածեք այն մասին, թե ամեն օր ինչպես պետք է հասանելի լինի ձեզ համար այդ ինֆորմացիան: Անգամ եթե ամպ ծառայության մատակարարը անբասիր հեղինակություն ունի և պահպանում է անվտանգության միջոցառումները, դուք պետք է ապահովեք ընկերության յուրաքանչյուր սարքի պաշտպանությունը, որը

բիզնես-ինֆորմացիան դարձնում է հասանելի: Դուք պետք է յուրաքանչյուր համակարգչի, նոութբուքի, սերվերի և բջջային սարքի համար պաշտպանական լուծում ապահովեք:

Միշտ զգոն եղեք

Դուք և ձեր աշխատակիցները պետք է հետևեք ձեր կազմած անվտանգության քաղաքականության ստանդարտ միջոցառումներին՝ ամպի լուծումներ օգտագործելիս: Օրինակ՝ պետք է շարունակել օգտագործել հուսալի գաղտնաբառեր՝ կանխարգելելու համար չհրահանգված հասանելիությունը, իսկ աշխատակիցները պետք է միջոցառումներ ձեռնարկեն իրենց բջջային սարքերը չկորցնելու համար:

Անհրաժեշտ է գնահատել տվյալների անվտանգության հնարավոր ռիսկերը և տեղեկացնել աշխատակիցներին պաշտպանական պարզ միջոցառումների մասին: Իրականում ամպ ծառայության օգտագործման դեպքում ձեր ինֆորմացիան հեռացված պահպանում է կողմնակի մատակարարը:

Ուշադիր եղեք ամպ պահոցները օգտագործելու պայմաններին

Ամպ ծառայությունների շուկայում ներկայացված են ամենատարբեր լուծումները: Ամպ պահոցներից շատերը նախատեսված են տնային օգտատերերի համար: Նման լուծումների համար անվտանգության ապահովումը չի եղել առաջնահերթ խնդիր, հետևաբար բիզնես-նպատակների համար դրանք հուսալի չեն:

Մատակարարին ընտրելիս պարզեք հետևյալը՝

→ *ամպում պահելիս, ում է պատկանելու ձեր բիզնես-ինֆորմացիան,*

→ *ինչ կլինի, եթե մատակարարը դադարեցնի գործունեությունը,*

  ↘ *ինֆորմացիան առաջվա պես հասանելի կլինի ձեզ համար,*

  ↘ *ընկերությունը կմատնվի պարապուրդի, եթե ինֆորմացիան մի մատակարարից փոխանցվի մեկ ուրիշի,*

  ↘ *կմնան արդյոք ձեր ինֆորմացիայի պատճենները առաջին մատակարարի մոտ և ինչ երաշխիքներ կան, որ դրանք կջնջվեն,*

→ *ինչպես կարելի է լուծարել պայմանագիրը,*

  ↘ *եթե դուք որոշեք լուծարել պայմանագիրը, ինչպես կարելի է տեղափոխել ձեր բիզնես-ինֆորմացիան,*

→ *որքանով են հուսալի այն համակարգիչները, որտեղ պահվում է ձեր ինֆորմացիան և մատակարարի հաղորդակցման համակարգերը, որոնց միջոցով հասանելի է լինելու ինֆորմացիան:*

  ↘ *Մատակարարը պետք է երաշխավորի, որ ձեզ համար ձեր ինֆորմացիան միշտ հասանելի է լինելու և որևէ անսարքություն չի խանգարելու ձեզ:*

  ↘ *Ներդրել է արդյոք մատակարարը անհրաժեշտ տեխնոլոգիաներ, որոնք ապահովում են համակարգչային համակարգերի վթարներից կամ հարձակումներից հետո արագ վերականգնումը՝ չանդրադառնալով ինֆորմացիայի անվտանգության և հասանելիության վրա:*

- ↘ *Ինֆորմացիան կորստից և չհրահանգավորված հասանելիությունից պաշտպանելու ինչ պաշտպանական մակարդակ է ապահովում մատակարարը: (Հիշեք, որ դուք էլ պետք է օգտագործեք պաշտպանական ծրագրային ապահովում բոլոր այն բջջային սարքերի համար, որոնցով հասանելի է այդ ինֆորմացիան):*

→ *Որտե՞ղ է պահվելու ձեր ինֆորմացիան*

- ↘ *Նորմատիվ և օրենսդրական պահանջները թույլատրում են ինֆորմացիան պահել երկրից դուրս:*

Ձեր երեխայի խնամքը դուք չեք վստահի մի մարդու, որին չեք վստահում: Նմանապես, եթե ձեզ անհանգստացնում է ձեր ընկերության անվտանգությունը՝ անհրաժեշտ է որոշ ժամանակ ծախսել ամպ ծառայության մատակարարին գնահատելու համար: Այսպիսով դուք վստահ կլինեք, որ ձեր անձնական և գաղտնի տվյալները հուսալի ձեռքերում են:

Ինֆորմացիայի և հավելվածների ամպ պահոց տեղափոխելու փաստարկները շատ համոզիչ կարող են լինել: Բայց նման քայլը պետք է անել շատ զգույշ: Ամպ տեխնոլոգիաները կարող են հեշտացնել ձեր աշխատանքի որոշ ասպեկտներ, կարող են բարդության լրացուցիչ մակարդակ ավելացնել աշխատելիս:

Ամպ տեխնոլոգիաների օգտագործումը չի ազատում գաղտնի ինֆորմացիայի անվտանգությունը ապահովելու պատասխանատվությունից: Գործարար ինֆորմացիայի պաշտպանությունը ձեր պարտականությունն է: Եթե ամպ պահոցը բավարար պաշտպանություն չունի, ապա որևէ խնդրի առաջացման դեպքում պատասխանատվությունը կրելու եք դուք:

Գլուխ 5
ՀԱՐՄԱՐ ՊԱՇՏՊԱՆԱԿԱՆ ԼՈՒԾՄԱՆ ԸՆՏՐՈՒԹՅՈՒՆԸ

Այս գլխում՝

- *Պաշտպանական ծրագրային ապահովման լավագույն մատակարարի ընտրությունը:*
- *Անհրաժեշտ աջակցության ապահովումը:*
- *Ինչպե՞ս կարող են փոխվել ընկերության պահանջները ինֆորմացիոն անվտանգության նկատմամբ:*
- *Պաշտպանության լավագույն մակարդակի ընտրություն:*

Եվ այսպես, դուք գնահատել եք ձեր ընկերության անվտանգության ռիսկերը և զրուցել եք աշխատակիցների հետ ինֆորմացիայի պաշտպանության անհրաժեշտության մասին: Այժմ պետք է ընտրել այնպիսի պաշտպանական ծրագրային լուծում, որը լավագույնս կապահովի ձեր ընկերության անվտանգությունը:

ՃԻՇՏ ՄԱՏԱԿԱՐԱՐԻ ԸՆՏՐՈՒԹՅՈՒՆԸ

ՏՏ պաշտպանելու համար շուկայում առկա ծրագրային արտադրանքից ընտրեք այն, որը ընկերության զարգացման հետ կարող է հարմարվել ընկերության պահանջներին:

Աջակցությունը պետք է բոլորին

Պարզեք մատակարարներից՝ինչ աջակցություն կարող եք ստանալ, եթե խնդիրներ առաջանան ապահովման ծրագրի հետ կապված կամ ընկերությունը դառնա հարձակման զոհ: Բարդ իրավիճակում զանգահարել և միանգամից օգնություն ստանալը ոչ միայն հուսադրում և հանգստացնում է, այլև օգնում է խնայել ժամանակը և արագ վերականգնել համակարգիչների աշխատանքը և բիզնես-գործընթացները:

Եթե մատակարարը առաջարկում է ինքնուրույն որոնել խնդրի լուծումը համացանցի իր գիտելիքների բազայում, իմացեք, որ դուք երկար ժամանակ չեք զբաղվի ձեր հիմնական գործով: Բոլորը գիտեն, որ նման տեխնիկական խնդիրները ծագում են ամենապատասխանատու պահին, օրինակ՝ կարևոր գործարքի համար մանրամասն առաջարկությունների ներկայացման վերջին օրը:

Փորձեք գտնել այն մատակարարին, որն աջակցություն է ցուցաբերում ձեզ հասկանալի լեզվով:

Պաշտպանական լուծումը ընտրելիս պետք է գտնել այն մատակարարին, որը անհրաժեշտ աջակցություն է ցուցաբերում: Շուկայում առկա են անվտանգությունն ապահովող մի քանի փաթեթային լուծումներ, որոնք ներառում են տարբեր տեխնոլոգիաներ՝ վնասատու ծրագրերի և ինտերնետ-սպառնալիքների դեմ պայքարի համար: Բայց երբ ձեր ընկերությունը մեծանա, այդ փաթեթները ձեզ այլևս չեն բավարարի:

→ *Կկարողանա ձեր մատակարարը առաջարկել այլ փաթեթ՝ ընդլայնված ֆունկցիաներով:*

→ *Արտադրանքը ունի համակարգչային ցանցի նոր*

Էլեմենտների (օրինակ՝նոր սերվերների)պաշտպանության ֆունկցիայի ավելացման հնարավորություն:

Այս հարցերը կարող են թվալ ոչ կարևոր: Բայց ընկերության ընդլայնման հետ այս հարցերը կազատեն ձեզ պարապուրդից և անվտանգությունը ապահովող արտադրանք մատակարարող նոր մատակարարի փնտրտուքից:

Կարճ ժամանակում հասեք ավելիին

Ցանկացած ընկերության համար կարևոր է, որ իր օգտագործած ծրագրային լուծումները կիրառման համար լինեն պարզ: Ոչ ոք չի ուզում շատ ժամանակ ծախսել պաշտպանական ծրագրային ապահովման համալարման և կառավարման վրա, եթե ավելի կատարյալ արտադրանքը հնարավոր է դարձնում պաշտպանության շատ պրոցեսներ ավտոմատացնել և ժամանակ խնայել այլ խնդիրների լուծման համար:

Օգտագործման մեջ պարզ լինելը շատ կարևոր է, հատկապես, եթե դուք չունեք հաստիքով աշխատող ՏՏ մասնագետներ: Եթե ձեր ընկերությունը ընդլայնվի և դուք վարձեք ՏՏ և անվտանգության մասնագետների, օգտագործման մեջ պարզ պաշտպանական ապահովումը կբարձրացնի նրանց աշխատանքի արտադրողականությունը:

Անվտանգության ղեկավարման պարզեցումը

Պաշտպանական ծրագրային ապահովման միջերեսը հաճախ անվանում են կառավարման բարձակ: Ինչպես ավտոմեքենան ունի տվիչների, ցուցիչների և փոխարկիչների վահանակ, այնպես էլ կառավարման բարձակը պետք է ապահովի արտադրանքի աշխատանքի մասին ինֆորմացիայի արագ հասանելիությունը, վերլուծի խնդիրները և հնարավոր դարձնի հա-

մալարումների փոփոխությունները: Ծրագրային ապահովման շատ մատակարարներ հոգ չեն տանում իրենց արտադրանքի օգտագործման հարմարավետության մասին:

Ինչ-որ մի պաշտպանական ծրագրային ապահովում օգտագործող օգտատեր ստիպված է անցնել մի բարձակից մյուսին, որպեսզի ղեկավարի պաշտպանության տարբեր տեխնոլոգիաներ: Հաճախ սա բացատրվում է նրանով, որ մատակարարը ձեռք է բերել տարբեր տեխնոլոգիաներ պաշտպանական արտադրանք մշակող այլ ընկերություններից: Որն էլ լինի պատճառը՝ կառավարման մի քանի բարձակ օգտագործելը դժվարեցնում է կառավարիչի աշխատանքը և ավելի շատ ժամանակ է պահանջում:

Անվտանգությունը ապահովող այլ լուծումները հնարավորություն են տալիս պաշտպանական լուծումների բոլոր տեխնոլոգիաները թերթել և համալարել մեկ միասնականացված կառավարման բարձակում: Նշանակում է պետք է յուրացնել մեկ միջերես, որտեղ ներկայացված են պաշտպանության բոլոր տեխնոլոգիաները, որոնք օգտագործվում են համակարգչային ձեր ցանցում:

Եթե դուք եք կառավարելու պաշտպանական ծրագրային ապահովումը, ապա կիրառման և կառավարման հարմարության շնորհիվ ավելի շատ ժամանակ կունենաք բիզնես-խնդիրներով զբաղվելու համար: Եթե դուք պաշտպանական ծրագրային ապահովման կառավարումը հանձնել եք հաստիքային կամ արտահաստիքային մասնագետի, կառավարման միասնական պարզ բարձակը կօգնի կրճատել ծախսերը և կբարձրացնի ծրագրի արդյունավետությունը:

Օգտակար հաշվետվություններ

Արտադրանքը, որը ճկուն կերպով կարողանում է հաշվետվություններ կազմել ձեր SS ենթակառուցվածքի անվտանգության վիճակի և խոցելի տեղերի մասին, օգնում է, որպեսզի արագ և մանրամասն պարզել SS անվտանգության ոլորտում առաջացած խնդիրները:

ԱՄԲԻՑԻՈՉ ԸՆԿԵՐՈՒԹՅՈՒՆ, ԹԵ ԸՆՏԱՆԵԿԱՆ ՓՈՔՐ ՁԵՌՆԱՐԿՈՒԹՅՈՒՆ՝ ՈՐՈՇԵՔ ՁԵԶ ԱՆՀՐԱԺԵՇՏ ՊԱՇՏՊԱՆՈՒԹՅԱՆ ՄԱԿԱՐԴԱԿԸ

Պետք է ժամանակ տրամադրել և մտածել ձեր ընկերության հեռանկարների մասին և ազնվորեն պատասխանել այն հացին, թե ինչ նպատակներ ունեք: Հաճելի է պատկերացնել, որ մի օր ձեր ձեռնարկությունը կդառնա միջազգային կորպորացիա և կմրցի շուկայի ազդեցիկ խաղացողների հետ: Բայց ամեն մեկը չէ, որ մտածում է այդպես:

Շատ են այն օրինակները, երբ խոհանոցում կամ ավտոտնակում սկիզբ առած նախաձեռնությունները վեր են ածվել համաշխարհային մեծության ընկերությունների:

Եթե ձեր բիզնեսի հիմնական նպատակը ձեր ընտանիքի արժանապատիվ բարեկեցությունն է՝ պետք չէ ամաչել: Կողմնորոշվելով, թե ձեզ ինչ է անհրաժեշտ, դուք կընտրեք թե անվտանգության և SS համար ինչ ներդրումներ պետք է կատարեք:

Դուք պետք է ընդամենը պատասխանեք հետևյալ հարցերին՝

- → *Ընկերությունների ո՞ր տիպին է պատկանում ձեր ընկերությունը:*
- → *Ինչպիսի՞ն եք տեսնում ձեր ընկերությունը մեկ տարի հետո և ապագայում:*

Այս հարցերի պատասխանները ունենալով՝ ձեզ համար պարզ կլինի ինֆորմացիայի պաշտպանության ոլորտում ինչպես են փոփոխվելու ձեր ընկերության պահանջները: Այսպիսով դուք կկարողանաք ընտրել պաշտպանական ծրագրային այն արտադրանքը, որը համապատասխանում է ձեր ընկերությանը և ժամանակի հետ կարող է հարմարվել փոփոխություններին:

Անվտանգության ապահովման ոչ ճիշտ լուծման ընտրությունը սարսափելի չէ, բայց լրացուցիչ ծախսեր է պահանջելու:

ՏԱՆ ՀԱՄԱԿԱՐԳՉԻ ԱՆՎՏԱՆԳՈՒԹՅՈՒՆԻՑ ՄԻՆՉԵՎ ԲԻԶՆԵՍԻ ՊԱՇՏՊԱՆՈՒԹՅՈՒՆ

Գոյություն ունեն տարբեր չափերի ընկերությունների համար պաշտպանական ծրագրային արտադրանքներ: Ճիշտ ընտրությունը կախված է մի շարք գործոններից:

Տնային համակարգչի պաշտպանության համար արտադրանքներ

Եթե ձեր ընկերության կազմավորման պահին նրա մասին տեղեկատվությունը պահվում էր ձեր անձնական նոութբուքում, հավանական է, որ դուք օգտագործում էիք անձնական համակարգիչների պաշտպանության լուծումներից մեկը: Շատ արտադրանքներ, որոնք նախատեսված են տնային օգտատերերի համար, համատեղում են վնասատու ծրագրային ապահովման պաշտպանության տեխնոլոգիաները և ինտերնետ-սպառնալիքների դեմ նորարարական մշակումները: Որոշ լուծումներ առաջարկում են լրացուցիչ պաշտպանություն ինտերնետ-բանկինգի և ֆինանսական առցանց այլ գործառույթների համար:

Եթե ընկերությունում աշխատում են քիչ թվով մարդիկ, ապա

տնային համակարգչի համար ընտրված պաշտպանական արտադրանքը իդեալական է: Շուկայում ներկայացված են նմանատիպ բազմաթիվ լուծումներ, պետք է համեմատել դրանց ֆունկցիաները և հնարավորությունները: Միայն հակավիրուսային պաշտպանությունը ապահովող լուծումը ժամանակակից բոլոր վտանգներին չի կարող դիմակայել:

Որպես կանոն, տնային օգտագործման համար նախատեսված պաշտպանական ծրագրային ապահովումը հարմար է այն ընկերությունների համար, որտեղ աշխատում է չորս մարդուց ոչ ավելին: Նման մոտեցումը ճիշտ է, եթե տվյալ արտադրանքի հավաստագիրը թույլ է տալիս այն օգտագործել կոմերցիոն նպատակներով: Տնային օգտատերերի համար նախատեսված լուծումների մեծ մասը դժվար է ղեկավարել, եթե դրանցից օգտվում են ընկերության 5 և ավելի աշխատակից: Նման արտադրանքները թույլ չեն տալիս արագ և հեշտությամբ կիրառել անվտանգության համալարումները և պարամետրերը ընկերության բոլոր նոութբուքերի, համակարգիչների և բջջային սարքերի վրա:

Եթե դուք նախատեսում եք ընդլայնել ձեր բիզնեսը, ապա ձեր SS ենթակառուցվածքը նույնպես ընդլայնվելու և բարդանալու է: Տնային օգտագործման համար ընտրած պաշտպանական լուծումը, որը չի ընդլայնվում ձեր ընկերության ընդլայնման հետ, ստիպված եք լինելու փոխարինել նորով: Այսինքն կատարելու եք ֆինանսական ծախս և ընդհատելու եք ընկերության աշխատանքը:

Անվճար հակավիրուսային ծրագրային ապահովում

Եթե դուք օգտագործում եք անվճար հակավիրուսային ծրագրային ապահովում, երբ ձեր ընկերությունը ընդարձակվի, հավանական է, որ կցանկանաք շարունակել օգտագործել այն:

Պետք է պարզել, թե անվճար ծրագրային ապահովումը ինչ հնարավորություններ ունի:

Արդյոք ունի այն բոլոր տեխնոլոգիաները, որոնք անհրաժեշտ են նոր սպառնալիքներից և արժեքավոր ինֆորմացիայի կորստից պաշտպանելու համար: Եթե արտադրանքը ներառում է միայն հակավիրուսային ֆունկցիաներ և մի քանի լրացուցիչ բաղկացուցիչներ ինտերնետ-սպառնալիքներից պաշտպանելու համար, ապա այն չի պաշտպանի ձեզ ժամանակակից բոլոր ռիսկերից:

Ծրագրային անվճար փաթեթներից շատերը նախատեսված չեն ընկերությունների համար՝ հավաստագրի պայմաններով արգելվում է դրանց կոմերցիոն նպատակներով օգտագործել: Այդ պատճառով որոշ անվճար պաշտպանական լուծումների կիրառումը բիզնեսում հակաօրինական է: Հաճախ անվճար ծրագրային ապահովման մատակարարը կարող է տուրք գանձել՝ այն կոմերցիոն նպատակներով օգտագործելու դեպքում:

Անվճար ստանալ շան ձագ

Դուք միշտ ուզել եք հովվաշուն պահել և հիմա դուք կարող եք իրագործել ձեր երազանքը՝ մեծ գումար չվճարելով: Բայց սա ցեղական շուն չէ, սակայն ձերն է և ստացել եք անվճար:

Անվճար է, բայց հոգս է, լրացուցիչ ծախսեր և տանը խառնակ վիճակ: Դուք հաշվի եք առել սրսկումների և անասնաբույժի այցելությունների ծախսերը, բայց չեք մտածել քանի-քանի իր է կրծոտելու այդ շունը:

Կյանքում շատ քիչ բան է լինում ձրի: Անվճար ծրագրային ապահովումը կարող է հանգեցնել առաջին հայացքից չերևացող ծախսերի: Օրինակ՝ կարող է ցույց տալ կողմնակի արտադրանքների գովազդը կամ առաջարկել գնել «պրեմիում» տարբերակը: Այդ ցուցանակները և ծանուցումները շեղում են մարդու ուշադրությունը և կարող են նվազեցնել ձեր աշխատակիցների արտադրողականությունը: Եթե ծրագրային ապահովումը չի օգտագործում նման մեթոդներ, ապա մատակարարի կողմից այս ծրագրային ապահովմանը աջակցելը շատ թանկ է:

Պաշտպանական լուծումներ խոշոր ընկերությունների համար

Գիտակցելով գոյություն ունեցող բոլոր վտանգները, հնարավոր է դուք որոշեք գնել ամենաբազմաֆունկցիոնալ լուծումը: Շատ ընկերություններ չեն գիտակցում, որ ծրագրային արտադրանքների ֆունկցիոնալությունը և օգտագործման պարզությունը փոխկապակցված են: Այն արտադրանքները, որոնք ունեն այն ֆունկցիաները և անհրաժեշտ են միայն խոշոր ընկերություններին, հնարավոր է ավելի դժվար է համալարել և ղեկավարել, քան նրանք, որոնք նախատեսված են փոքր բիզնեսի համար:

Այդ պատճառով ոչ մեծ ընկերությունները, որոնք ընտրել են բազմաֆունկցիոնալ ծրագրային արտադրանքը, բարդացնում են իրենց վիճակը, քանի որ տարիներ են պետք ընկերության աճի համար և աճելուց հետո միայն ընկերությանը պետք կգա վաղօրոք ընտրած պաշտպանական ծրագրային ապահովումը: Մյուս կողմից ձեր մատակարարը ընկերության աճի հետ կօգնի լուծել անվտանգության խնդիրները:

Խոշոր ընկերությունների համար պաշտպանական լուծումները կարող են պարունակել առաջադեմ տեխնոլոգիաներ բարդ միջավայրերի անվտանգությունը ապահովելու համար: Բայց եթե ձեր SS ցանցը համեմատաբար պարզ է և մտադիր չեք այն ընդլայնել, ապա գնելով այդ լուծումը, դուք վճարելու եք ֆունկցիաների համար, որոնք, հավանական է, երբեք չեք օգտագործելու: Անվտանգության ապահովման բարդ լուծումը կարող է օգտագործման համար էլ բարդ լինի: Առաջին համալարումից սկսած մինչև ամենօրյա ղեկավարումը կարող է պահանջել շատ ժամանակ և հմտություններ, որոնք ոչ մեծ ընկերությունները չունեն: Կորպորատիվ մակարդակի լուծումների համար ընկերությունը պետք է ունենա համապատասխան ռեսուրսներ և հաստիքով աշխատող որակավորված SS մասնագետներ:

Պրեսյումերների մակարդակի անվտանգություն

Պրոսյումեր տերմինը ներմուծել են շուկայագետները (մարկետոլոգները), ծագում է անգլերեն «prosumer» բառից: Սրանք այն կոմպետենտ օգտատերերն են, որոնք հանգամանքների բերումով աշխատավայրում կատարում են SS ադմինիստրատորի ֆունկցիաներ:

Պրոսյումերների համար նախատեսված արդյունավետ և ղեկավարման համար հարմար լուծումները լրացնում են այն բացը, որ կա տնային օգտատերերի համար ստեղծված և պարզ ղեկավարվող արտադրանքների և կորպորատիվ լուծումների միջև, որոնք բարդ է համալարել և ղեկավարել:

Այսպիսով պրոսյումերների համար արտադրանքները միավորում են բիզնեսի համար անհրաժեշտ հեշտ ղեկավարվող ֆունկցիաները: Սա կարևոր է այն ընկերությունների համար, որտեղ չկան SS անվտանգության մասնագետներ: Եթե արտադրողները կարողանան հասնել այդ հավասարակշռությանը, պրոսյումերների համար պաշտպանական արտադրանքները ոչ մեծ ընկերությունների համար լավագույն լուծումն են:

Նկատելի տարբերություն կա փոքր բիզնեսի համար մշակած արտադրանքների և կորպորատիվ լուծումների միջև: Եթե արտադրողը իր արտադրանքի փաթեթավորումն է միայն փոխել և վաճառում է որպես արտադրանք պրոսյումերների համար, այսպիսի լուծման օգտագործումը կլինի բարդ և ժամանակատար:

Անկախ ձեր ընկերության չափից, ընտրեք այն մատակարարին, որը հաշվի է առել ձեր կազմակերպության տիպի կազմակերպությունների պահանջները և մշակել է համապատասխան ծրագրային լուծում:

Կորպորատիվ լուծումներ պրոսյումերների համար

Իրականում ամեն ինչ ավելի բարդ է: Խոշոր ընկերությունների համար նախատեսված որոշ արտադրանքներ հարմար են փոքր բիզնեսի համար: Ճիշտ է, որ այն արտադրանքները, որոնք

մշակվել են առանց հաշվի առնելու փոքր ընկերությունների յուրահատկությունները, հարմար են այն կազմակերպությունների համար, որոնք չունեն ներքին ռեսուրսներ SS անվտանգությունը սպասարկելու համար: Բայց կան բիզնեսի պաշտպանության համար արտադրանքներ, որոնք հիմնված են պարզ մոդուլային ճարտարապետության վրա:

Այդպիսի լուծումները կարող են ներառել արտադրանքի մի քանի մակարդակ, որոնք առաջարկում են պաշտպանական տեխնոլոգիաների տարբեր կոմբինացիաներ: Ամենացածր մակարդակը ապահովում է բազային պաշտպանությունը, որը հարմար է պարզ SS ցանցերի համար: Ամեն հաջորդ մակարդակը ավելացնում է պաշտպանական նոր տեխնոլոգիաներ, իսկ ամենաբարձր մակարդակը նախատեսված է կորպորատիվ բարդ SS միջավայրերի համար և ներառում է մի քանի օպերացիոն համակարգեր և բջջային պլատֆորմներ, վիրտուալ միջավայրերի անվտանգությունը ապահովող հատուկ ֆունկցիաներ, ինտերնետ-անցախուցերը և փոստային սերվերները պաշտպանող տեխնոլոգիաներ և այլ հնարավորություններ:

Այսպիսի մոդուլային արտադրանքները հնարավորություն են տալիս ընկերություններին օգտագործել պաշտպանական լուծումներ, որոնք բիզնեսի ընդլայնման հետ ընդարձակվում են:

Տարբեր ընկերություններ SS անվտանգության նկատմամբ տարբեր պահանջներ ունեն: Առաջարկների բազմազանության մեջ պետք է ընտրել այն, որը համապատասխանում է ձեր պահանջներին:

Գլուխ 6
ՏԱՍԸ ՀԱՐՑ, ՈՐՈՆՔ ԿՕԳՆԵՆ ՁԵԶ

Այս գլխում՝

- *Ընկերության պահանջների որոշակիացում:*
- *Իրավական պարտականությունների գնահատում:*
- *Անվտանգության քաղաքականության ընտրություն:*

Այս տասը հարցը կօգնեն որոշել, թե ինչ է պետք ձեր ընկերությունը կիբեռհարձակումներից, վնասատու ծրագրային ապահովումից և SS անվտանգության այլ ռիսկերից պաշտպանելու համար:

→ *Դուք գնահատե՞լ եք ձեր ընկերության անվտանգության հավանական ռիսկերը և որոշե՞լ եք, թե որ համակարգիչները և տվյալները պաշտպանության կարիք ունեն:*

→ *Բացի համակարգիչներից անհրաժեշտ է արդյո՞ք պաշտպանել բջջային սարքերը, այդ թվում BYOD շրջանակում:*

→ *Դուք գիտե՞ք ձեր ընկերության նորմատիվ և իրավական պարտականությունները գաղտնի ինֆորմացիային պահպանման հարցում:*

→ *Դուք որոշե՞լ եք պաշտպանության հիմնական կանոնները, որոնք կօգնեն ձեր ընկերությանը պաշտպանել ինֆորմացիան, համակարգիչները և այլ սարքեր:*

→ *Դուք ներդրե՞լ եք ուսուցանող ծրագիր, որը պետք է հրավիրի աշխատակիցների ուշադրությունը ինֆորմացիայի*

պաշտպանության խնդրին և մղի նրանց պահպանել SS անվտանգության կանոնները:

→ *Դուք վերլուծե՞լ եք շուկայում մատչելի պաշտպանական ծրագրային արտադրանքները հետևյալ սկզբունքներով՝ օգտագործման համար պարզ, պաշտպանության մակարդակները, անվտանգության պահանջներին հարմարվելը:*

→ *Պաշտպանական ծրագրային ապահովման ձեր ընտրած մատակարարը առաջարկու՞մ է աջակցության մակարդակ ձեզ հասկանալի լեզվով:*

→ *Ձեզ պե՞տք են ինտերնետ-բանկինգի և ֆինանսական առցանց գործառույթների լրացուցիչ պաշտպանության համար անվտանգության ֆունկցիաներ:*

→ *Դուք նախատեսու՞մ եք օգտվել ամպ պահոցներից, ստուգել եք պայմանագրի պայմանները՝ այդ թվում ինֆորմացիայի պաշտպանվածության աստիճանը:*

→ *Դուք ընտրե՞լ եք ծրագրային արտադրանք, որը պաշտպանում է ձեր համակարգիչները և բջջային սարքերը, որոնք օգտագործում է ձեր ընկերությունը ամպում պահվող ինֆորմացիային հասնելու համար:*

Համոզվե՛ք, որ ձեր ընկերության SS համակարգերը պաշտպանված են հուսալի ծրագրային արտադրանքով:

ԱՇԽԱՏԱՆՔԸ ԿԱՆԳՆԵ՞Լ Է

Աշխատանքային համակարգչում եղած ընդամենը մեկ վիրուսը կարող է ջնջել բոլոր արժեքավոր տվյալները, հափշտակել բանկային հաշվի գումարները և վտանգել ողջ բիզնեսը: «Կասպերսկի Լաբորատորիա»-ի լուծումների հետ ձեր տվյալները, ֆինանսները և բիզնեսն ապահով կլինեն:

ԲԻԶՆԵՍ ԱՌԱՆՑ ՍՊԱՌՆԱԼԻՔՆԵՐԻ

kaspersky.ru

KASPERSKY lab

Ընկերության պաշտպանությունը վնասաբեր ծրագրերից և կիբեռգրոհներից

Բոլոր ընկերությունների՝ սկսնակներից մինչև միջազգային կորպորացիաների կախվածությունը համակարգիչներից և շարժական սարքերից գնալով մեծանում, իսկ դա նշանակում է, որ դրանք ավելի ու ավելի խոցելի են դառնում կիբեռհանցագործների գրոհների առջև: Այս գրքում խոսվում է այն մասին, թե ինչպես արդյունավետ պաշտպանել բիզնես տեղեկատվությունը, այդ թվում ընկերության հաճախորդների գաղտնի տվյալները, պաշտպանել ընկերության համակարգիչները և շարժական սարքերը վիրուսներից և այլ վնասաբեր ծրագրային ապահովումից: Մեր խորհուրդները և հանձնարարականները կօգնեն ձեզ ավելի քիչ ժամանակ ծախսել անվտանգության, ապահովման, և ավելի շատ՝ բիզնեսի վարման համար:

- ***Իմացեք SS-անվտանգության հետ կապված ռիսկերի մասին** - ինչից պետք է զգուշանա ձեր ընկերությունը*
- ***Ծանոթացեք սպառնալիքներին** – իմացեք, թե ինչպես են հանցագործները ընտրում թիրախներ հարձակման համար*
- ***Պլանավորեք պաշտպանությունը** – խուսափեք տարածված սխալներից*
- ***Պաշտպանեք ձեր տվյալները** – գինվեք օգտագործման համար հարմար պաշտպանական ծրագրային ապահովմամբ*

Այս գրքից կիմանաք.

- ***գրոհների ինչ մեթոդներ են կիրառում կիբեռհանցագործները***
- ***ինչպես ապահովել արժեքավոր տեղեկատվության պահպանությունը***
- ***ինչպես ընտրել հենց ձեր ընկերությանը համապատասխանող ծրագրային ապահովում***

***Ջորջիանա Գիլմորն** ունի SS-արդյունաբերությունում ավելի քան 20 տարիների փորձ: Ջորջիանան գբաղեցնում է «Կասպերսկի Լաբորատորիա»-ի Կորպորատիվ մարկետինգային ծրագրերի և արշավների գծով տնօրենի պաշտոնը:*

***Պիտեր Բիրդմորը** «Կասպերսկի Լաբորատորիա»-ում աշխատում է 2008թ.-ից: Տիրապետում է SS-մարկետինգի ոլորտում և արտադրության կառավարման խորը գործնական գիտելիքների: Պիտերը ղեկավարում է արտադրանքի մարկետինգի բաժինը:*