Գաղտնի տեղեկատվության պաշտպանությունը կազմակերպությունների 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:

Սկզբում պետք է պատասխանել հետևյալ հարցերին՝

- որտե՞ղ է պահվում մեր բիզնեսինֆորմացիան,
- 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 բիզնեսինֆորմացիայի պաշտպանության միջոցները
- Որքանո՞վ են ձեռնարկվող միջոցառումները հա մապատասխանում իմ ոլորտում և այս մեծության ընկերության համար ընդունված նորմերին (բիզնեսի
- ընդլայնման հետ ստիպված եք լինելու ինֆորմացիայի պաշտպանության մակարդակը բարձրացնելու հա մար միջոցներ ծախսել):
- Կհամաձայնվի՞ դատարանը, որ իմ ընկերությունը կիրառում է պաշտպանության անհրաժեշտ միջո ցառումները:
- Որքանո՞վ է հավանական, որ իմ ընկերությունը կտուժի գաղտնի ինֆորմացիայի արտահոսքից:

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

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 տարրա կան 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 ժա մանակակից 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 քա ղաքականության 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 WiFi ցանցերի օգտագործման ռիսկերը և դրանց կանխարգելման միջոցները,
  - նպատակային ֆիշինգային հարձակումների բացա հայտումը,
  - ինչպես կանդրադառնա բջջային սարքի կորուստը ընկերության անվտանգության վրա:
- Ապահովեք անվտանգության քաղաքականության իրագործումը, օրինակ՝ ձեռնարկեք միջոցներ, որպեսզի երաշխավորվի հուսալի գաղտնաբառերի օգտագործումը բիզնեսինֆորմացիայի, բանկային հաշիվների հա սանելիության 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 պա կաս։

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։

Ամպային տեխնոլոգիաներ

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

Երբեմն ոչ մեծ կազմակերպությունները ավելի արագ են փո խառնում 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։

Ձեր ինֆորմացիայի պահպանված լինելը ձեր խնդիրն է

Եթե դուք ուզում եք բիզնեսինֆորմացիայի մի մասը կամ ինչոր հավելված տեղափոխել ամպի մեջ՝ հիշեք, որ դրանց անվտանգության համար շարունակում է պատասխա նատվություն կրել ձեր ընկերությունը։ Բացի այդ ամպի մեջ պահելը չի նշանակում, որ ձեր բիզնեսինֆորմացիան 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 բիզնեսինֆորմացիան դարձնում է հասանելի։ Դուք պետք է յուրաքանչյուր

համակարգչի, նոութբուքի, սերվերի և բջջային սարքի համար պաշտպանական լուծում ապահովեք։

Դուք և ձեր աշխատակիցները պետք է հետևեք ձեր կազմած անվտանգության քաղաքականության ստանդարտ միջո ցառումներին՝ 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 հնա րավոր ռիսկերը և տեղեկացնել աշխատակիցներին պաշտպա նական պարզ միջոցառումների մասին։ Իրականում ամպ ծառայության օգտագործման դեպքում ձեր ինֆորմացիան հե ռացված պահպանում է կողմնակի մատակարարը։

Ուշադիր եղեք ամպ պահոցները օգտագործելու պայմաններին

Ամպ ծառայությունների շուկայում ներկայացված են ամե նատարբեր լուծումները։ Ամպ պահոցներից շատերը նա խատեսված են տնային օգտատերերի համար։ Նման լուծումների համար անվտանգության ապահովումը չի եղել առաջնահերթ խնդիր, հետևաբար բիզնեսնպատակների հա մար 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 բիզնեսինֆորմացիան,
- որքանով են հուսալի այն համակարգիչները, որտեղ պահվում է ձեր ինֆորմացիան և մատակարարի հաղորդակցման համակարգերը, որոնց միջոցով հա սանելի է լինելու ինֆորմացիան։
    - Մատակարարը պետք է երաշխավորի, որ ձեզ հա մար ձեր ինֆորմացիան միշտ հասանելի է լինելու և որևէ անսարքություն չի խանգարելու ձեզ։

- Ներդրել է արդյոք մատակարարը անհրաժեշտ տեխնոլոգիաներ, որոնք ապահովում են հա մակարգչային համակարգերի վթարներից կամ հարձակումներից հետո արագ վերականգնումը՝ չանդրադառնալով ինֆորմացիայի անվտանգության և հասանելիության վրա։
- Ինֆորմացիան կորստից և չհրահանգավորված հասանելիությունից պաշտպանելու ինչ պաշտպա նական մակարդակ է ապահովում մատակարարը։ (Հիշեք, որ դուք էլ պետք է օգտագործեք պաշտպա նական 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 գնա հատելու 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 պարտա կանությունն է։ Եթե ամպ պահոցը բավարար պաշտպանություն չունի, ապա որևէ խնդրի առա ջացման դեպքում պատասխանատվությունը կրելու եք դուք։
Ամպ տեխնոլոգիաների օգտագործումը չի ազատում գաղտնի ինֆորմացիայի անվտանգությունը ապահովելու պատասխանատվությունից։ Գործարար ինֆորմացիայի պաշտպանությունը ձեր պարտա կանությունն է։ Եթե ամպ պահոցը բավարար պաշտպանություն չունի, ապա որևէ խնդրի առա ջացման դեպքում պատասխանատվությունը կրելու եք դուք։

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 ինտերնետսպառնալիքների 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։
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 SS մասնագետներ։ Եթե ձեր ընկերությունը ընդլայնվի և դուք վարձեք SS և անվտանգության մասնագետների, օգտագործման մեջ պարզ պաշտպանական ապահովումը կբարձրացնի նրանց աշխատանքի արտադրողականությունը։
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 համալարումների 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:

Դուք պետք է 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:

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:
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։

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։

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, ինտերնետանցախուցերը և փոստային սերվերները պաշտպանող տեխնոլոգիաներ և այլ հնարավորություններ: Այսպիսի մոդուլային արտադրանքները հնարավորություն են տալիս ընկերություններին օգտագործել պաշտպանական լուծումներ, որոնք բիզնեսի ընդլայնման հետ ընդարձակվում են: