DIGIFENCE
TECHNOLOGY

27/4 Azatutyan Avenue
Yerevan 0014 Armenia
(374) 11 48 48 48
/digifence.tech
info@digifence.am
www.digifence.tech

Կիբեռանվտանգության ձեռնարկատիրական մակարդակ

▼ 01

NIST կիբեռանվտանգության կառուցվածք

ՆԿԱՐԱԳՐՈՒԹՅՈՒՆԸ

Հիմա, ավելի քան երբևէ, կազմակերպությունները պետք է բալանսի բերեն արագորեն աճող կիբեռ սպառնալիքների մակարդակը՝ բիզնես պահանջների կատարման անհրաժեշտությանը: Կազմակերպություններին օգնելու համար կառավարել իրենց կիբեռանվտանգության ռիսկը, NIST-ը առաջարկում է շահագրգիռ կողմերին զարգացնելու Կիբեռանվտանգության կառուցվածք, որը կհասցեագրի սպառնալիքները և կաջակցի բիզնեսին: Մինչդեռ կառուցվածքի առաջնային շահառու կողմերը ԱՄՆ մասնավոր սեկտորի սեփականատերեր են և կրիտիկական ենթակառուցվածքի օպերատորները, դրա օգտագործողները աճել են աշխարհով մեկ:

Կառուցվածքը ինտեգրում է արդյունաբերության ստանդարտներ և լավագույն փորձեր՝ օգնելու կազմակերպություններին կառավարել իրենց կիբեռանվտանգությանն ռիսկերը: Դա բերում է միահամուռ լեզվի, որը թույլ է տալիս կազմակերպության բոլոր մակարդակների անձնակազմին և մատակարարման շղթայի բոլոր կետերին՝ զարգացնելու համատարած հասկացողություն իրենց կիբեռանվտանգության ռիսկերի մասով: NIST-ը աշխատել է մասնավոր սեկտորի և կառավարության հմուտ մասնագետների հետ՝ ստեղծելով կառուցվածք, որը գործի է դրվել 2014թ -ից: Ջանքն այնքան տեղին էր, որ ԱՄՆ Կոնգրեսը անվանեց այն NIST-ի պատասխանատվություն Կիբեռանվտանգության բարելավման 2014-ի Ակտում:

Կառուցվածքը ոչ միայն օգնում է կազմակերպություններին հասկանալ իրենց կիբեռանվտանգության ռիսկերը (սպառնալիքները, խոցելիությունները և ազդեցությունները), այլև օգնում են հասկանալ, թե ինչպես նվազեցնել այդ ռիսկերը հատուկ միջոցներով: Կառուցվածքը նաև օգնում է արձագանքելու կիբեռանվտանգության պատահարներին և վերականգնվելու դրանցից՝ վերլուծելով դրանց հիմնային պատճառները և հաշվի առնելով նրանց բարելավումներ անելու կարողությունը: Ամբողջ աշխարհի կազմակերպությունները (ինչպես օրինակ՝ JP Morgan Chase, Microsoft, Boeing, Intel, Bank of England, Nippon Telegraph and Telephone Corporation, Ontario Energy Board) գրկաբաց ընդունեցին կառուցվածքի կիրառությունը:

NIST-ը շարունակում է խրախուսել կառուցվածքի կիրառումը և դրա իրականացումը տեղական և համաշխարհային շուկաներում: NIST-ը նաև շարունակում է աշխատել արդյունաբերության և այլ շահագրգիռ կողմերի հետ՝ հաստատելու, որ կառուցվածքի թարմացումները պահպանում են իրենց համապատասխանությունը և օգտակարությունը կազմակերպությունների լայն շրջանակի համար:

▼ 02

ISO 27001 Տեղեկատվական անվտանգության կառավարման համակարգ

ՆԿԱՐԱԳՐՈՒԹՅՈՒՆԸ

ISO/IEC 27000 ստանդարտների խումբը օգնում է կազմակերպություններին անվտանգ պահպանել տեղեկատվական ակտիվները: Այս ստանդարտների խմբի կիրառումը օգնում է կազմակերպություններին կառավարել ակտիվների անվտանգությունը, ինչպիսիք են՝ ֆինանսական տեղեկատվությունները, մտավոր սեփականությունը, աշխատակցի անձնական տվյալները կամ երրորդ անձանց կողմից տրամադրված տեղեկատվությունը:

ISO/IEC 27001 տեղեկատվական անվտանգության կառավարման համակարգի (ՏԱԿՀ) պահանջներ ապահովող ամենաճանաչված ստանդարտն է:

ՏԱԿՀ-ը սիստեմատիկ մոտեցում է՝ կառավարելու զգայուն կազմակերպությունների տեղեկատվությունը այնքան մինչդեռ այն մնում է անվտանգ: Այն ներառում է մարդկանց, գործընթացներն ու ՏՏ համակարգերը՝ կիրառելով ռիսկի կառավարման գործընթացը:

Այն կարող է օգնել փոքր, միջին և մեծ բիզնեսներին ցանկացած սեկտորում պահպանել տեղեկատվական ակտիվներն անվտանգ: Ինչպես այլ ISO կառավարման համակարգի ստանդարտները, ISO/IEC 27001-ի հավաստագրումը հնարավոր է, սակայն պարտադիր չէ (Հայաստանի Հանրապետության Կենտրոնական բանկը պարտադրում է համապատասխանությունը ISO/IEC 27001-ին): Որոշ կազմակերպություններ ընտրում են ստանդարտի կիրառումը լավագույն փորձից օգուտ քաղելու նպատակով, մինչդեռ մնացածը որոշում են, որ նրանք ևս ցանկանում են հավաստագրված լինել հաճախորդներին հավաստիացնելու ստանդարտի պահանջների պահպանման վերաբերյալ:

Աշխարհի շատ կազմակերպություններ հավաստագրված են ISO/IEC 27001 ստանդարտով: