ISSN 2181-3187

NIMA UCHUN TASHKILOT DLP TEXNOLOGIYASIGA MUHTOJ

Xasanov Sardorbek Iqboljon óg'li
Muhammad al Xorazmiy nomidagi
Toshkent Axborot Texnologiyalari Universiteti
Farg'ona filiali magistri

Bizga ma'lumki korxonalarda axborot xavfsizligi qat'iy ta'minlanishi zarur. Mana shu vaziyatda bizga DLP(dddataaa leak prevention) texnologiyasi yordam beradi. Uning ma'nosi ma'lumotlarni tashkilot ichidan tashqariga chiqib ketishini ta'minlashdir. Ma'lumotlar chiqishini oldini olish (DLP) texnologiyasi tashkilotga o'zlarining maxfiy korporativ ma'lumotlarini kompaniya ichida saqlashga va qasddan yoki ehtiyotsiz harakatlar natijasida ma'lumotlar yo'qotilishini cheklashga yordam beradi.

DLP texnologiyasi sizga ma'lumotlar va hujjatlarni boshqarish imkonini beradi, ularni ma'lum bir kontent (masalan, shaxsiy identifikatsiya raqami) bilan tavsiflaydi va keyin muayyan siyosatlarni amalga oshiradi.

Axborot har bir tashkilotda muhim ishlab chiqarish vositasidir. Tashkilotning uzluksizligini ta'minlash tashkilotda mavjud bo'lgan barcha ma'lumotlarga alohida e'tibor berishni talab qiladi. Harakatlarning oqibatlaridan xabardor bo'lmaslik va uchinchi shaxslarning qasddan urinishlari tufayli ma'lumotlarning bir qator yo'llar orqali yo'qolishi tendentsiyasi mavjud.

1. Bu qism ham DLP qisqartmasi bilan ammo ma'nosi boshqa. Data loss protection (DLP) Ma'lumotlarni yo'qotishdan himoya qilish. Hujjatlarga tayinlangan xususiyatlar ma'lumotlarni ruxsatsiz tashuvchilarda saqlash yoki ularni tashqi qabul qiluvchilarga yuborishni imkonsiz qilish uchun asos bo'lib xizmat qiladi. Bu ma'lumotlarni yo'qotish ehtimolini sezilarli darajada kamaytiradi. Aytaylik, shaxsiy yoki korporativ moliyaviy ma'lumotlarni o'z ichiga olgan maxfiy hujjat "Faqat ichki foydalanish uchun" sifatida tavsiflangan bo'lsa, unda ushbu hujjatni USB flesh-diskda va hokazolarda saqlash mumkin emas. Siz qoidalarni, masalan, amaldagi qonunchilik va me'yoriy talablar yoki tashkilotingizdagi mavjud ma'lumotlarni tasniflash siyosati asosida o'rnatasiz.

2. Aniqlash(detection). Shuningdek, siz DLP texnologiyasidan ma'lumotlar do'koningizdagi kontent asosida ma'lumotlaringizni tahlil qilish uchun foydalanishingiz mumkin. Bu sizga maxfiy ma'lumotlaringizning joylashuvi haqida tushuncha beradi. DLP texnologiyasi, shuningdek, qaysi huquqlar buzilganligi haqida tushuncha beradi. Agar xohlasangiz, ma'lumotlar yo'qolishi xavfini kamaytirish va cheklash uchun profilaktika choralarini kiritishingiz mumkin.

ISSN 2181-3187

3. Ogohlik va trening(awareness & training). DLP texnologiyasining oldini olish va aniqlash xususiyatlari xodimlarning ma'lumotlar muammolari haqida xabardorligini oshirishi mumkin. Xodimlarni siyosat va hodisalar haqida hisobot kabi masalalardan xabardor qilish, ayniqsa ehtiyotsizlik tufayli ma'lumot yo'qolishining oldini olish uchun ishlaydi.

Tashkilotlar uchun DLP. Oxir-oqibat DLP tarmoqni almashtirishdan tortib xavfsizlik devorigacha mavjud resurslar va xavfsizlik choralariga kiritilgan butun tashkilot texnologiyasiga aylanadi. Masalan, federativ IRM bilan integratsiyalashganda, murakkab zanjirli tashkilotlarda yuqori xavfsizlik darajasiga olib kelishi mumkin bo'lgan juda kuchli manbadir. DLP o'z tashkilotiga qo'yiladigan oddiy paket emas, agar u to'liq xavfsizlik texnologiyasida to'g'ri joylashtirilgan bo'lsa, u ajralmas tashkilotning qismiga aylanadi.

Yuqoridagi ma’lumotlardan xulosa shundaki tashkilot uchun ma’lumotlar ombori birinchi o’rinda turuvchi omil hisoblanadi.

Foydalanilgan adabiyotlar:

1. G’aniyev S. K. ,Karimov M. M., Tashev K. A. AXBOROT XAVFSIZLIGI Toshkent 07
2. S.S. Qosimov Axborot texnologiyalari xaqida o’quv qo’llanma Toshkent 07
3. G’aniyev S.K.Karimov M.M. Hisoblash tizimlari va tarmoqlarida axborot xavfsizligi TDTU 03
4. http://www.kaspersky.ru
5. Data leak prevention technology. https://www.traxion.com/services/cyber-security-services/preventive-detective-security-services/data-leak-prevention/