AXBOROT XAVFSIZLIGI XAVFLARINI TAHLIL QILISH UCHUN IERARXIK AKTIVLARNI BAHOLASH USULI

Muxtorov Farrux Muxammadovich
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Farg‘ona filiali, Telekommunikatsiya texnologiyalari va kasbiy ta’lim fakulteti dekani

Umarov Abdumuxtor Maxammad o‘g‘li
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Farg‘ona filiali, 1-bosqich magistr
Abdumuxtorfdu94@gmail.com

ANNOTATSIYA

Ushbu maqola ierarxiyaga asoslangan aktivlarni baholash usulini taklif qiladi. Usul axborot xavfsizligini boshqarish loyihalari jarayonida yo‘l qo‘yilgan keng tarqalgan xatolarni minimallashtirish uchun mo‘ljallangan.

Usulni qo‘llash hali amalga oshirilmagan, ammo u jarayonlarni osonlashtirishi va xatolar sonini kamaytirishi mumkinligiga ishoniladi.

Kalit so‘zlar: Axborot xavfsizligi xavfini tahlil qilish, baholash aktivlar.

ABSTRACT

This article proposes a hierarchy-based asset valuation method. The method is designed to minimize common mistakes that have been made in the course of information security management projects.

The application of the method has not yet been carried out, but it is believed that it can facilitate processes and reduce the number of errors.

Keywords: Information security risk analysis, assessment assets.

KIRISH: Axborot texnologiyalari bugungi kunda biznes yuritishning ajralmas qismiga aylandi. Axborot texnologiyalari mustaqil paketlangan ilovalardan bugungi kunning o‘zaro bog‘langan mobil tizimlariga aylandi. Ushbu evolyutsiya barcha turdagi korxonalar tomonidan axborot texnologiyalaridan keng foydalanishga olib keldi. Yigirma yildan ko‘proq vaqt oldin, har bir tashkilotda biznes jarayonlarining aksariyati qog'ozda hujjatlashtirilgan. Hozirgi vaqtda deyarli har bir biznes jarayoni axborot texnologiyalariga bog'liq. Shu sababli, axborot tizimlari operatsion samaradorlikni oshirish vositasi sifatida boshlangan bo‘lsa-da, keyinchalik ular tashkilotning mavjudligi uchun ajralmas rolga ega bo‘ldi.

ADABIYOTLAR TAHLILI VA METODOLOGIYA

Aktivlarni identifikatsiya qilish va baholash risklarni tahlil qilishda bajarilishi kerak bo‘lgan eng muhim jarayondir. To‘g'ri aniqlangan va baholanmagan aktivlarsiz, risklarni tahlil qilish natijalari noto‘g'ri qarorlar qabul qilishga olib keladi. Axborot xavfsizligi sohasidagi noto‘g'ri qarorlar bevosita ta'sir qilishi mumkin. Adabiyotlarda aktivlarni aniqlash va baholashning tayyor va qo‘llanilgan usullari mavjud, ammo bu usullar murakkab va amaliy axborot xavfsizligini boshqarish loyihalari uchun mos emas. Axborot texnologiyalarining keng qo‘llanilishi biznesni doimiy va tez o‘zgartiradi. Axborot texnologiyalari tashkilotlarga yangi tahdidlarni ham keltirib chiqaradi. Xatarlarni tahlil qilish to‘g'ri qaror qabul qilish va ular bilan kurashish uchun muhim vositadir. Tashkilotlarda axborot tizimlaridan umumiy foydalanish bilan bir qatorda, axborot tizimlariga tahdid va hujumlar ham tez suratlar bilan o‘sdi.

Xavfsizlik hodisalari va tahdidlari soni kundan kunga ortib bormoqda. Aksariyat biznes operatsiyalari axborot texnologiyalariga bog'liq bo‘lganligi sababli, axborot texnologiyalariga tahdid biznesning o‘ziga tahdidni anglatadi. Moliyaviy ta'sirdan tashqari, xavfsizlik hodisalari nomoddiy aktivlarga ta'sir qilishi mumkin.

Axborot xavfsizligi hodisalari ishonchni yo‘qotish va moliyaviy yo‘qotish bo‘lishi mumkin. Axborot texnologiyalari har qachongidan ham muhimroq bo‘lganligi sababli va tashkilotlar axborot tizimlariga ko‘proq tayanadi, buning uchun mas'uliyat yuklaydi.

Axborot xavfsizligi yuqori rahbariyat uchun ustuvor vazifalardan biriga aylandi. ISO/IEC 27001:2005 standartida menejment xavfni qabul qilish mezonlarini belgilash orqali tashkilotning axborot xavfsizligiga sodiqligini namoyish etadi.

NATIJALAR

Ierarxiyalarni tahlil qilish usuli muammoni oddiyroq tarkibiy qismlarga ajratish va juft taqqoslashda mutaxassisning mulohazalari ketma-ketligini keyingi qayta ishlashdan iborat. Ierarxiyalarni tahlil qilish usuli aniqlik va ko‘p mezonlar sharoitida qaror qabul qilishni asoslashga xizmat qiladi. Ko‘p mezonli tanlov muammosining eng oddiy to‘liq ierarxiyasi uchta darajani o‘z ichiga oladi: aktiv, zaiflik, tahdid.

Xavf funktsiyasi uchta o‘zgaruvchiga ega: aktivlar, zaiflik va tahdid. Xavf funksiyasining birinchi kiritilishi, aktiv, ISO/IEC 27001:2005 standartida tashkilot uchun qimmatli bo‘lgan har qanday narsa sifatida aniqlanadi. Aktivning qiymatini aniqlash xavf tahlilining muhim qismidir.

Zaiflik - bu axborot tizimiga hujum qilish tahdidi bilan foydalanilishi mumkin bo‘lgan aktivdagi nuqson. Dasturiy ta'minot va apparat kompaniyalari raqobatbardosh bo‘lish uchun axborot texnologiyalaridagi tez o‘zgarishlarni moslashtirishga harakat qilmoqdalar, ammo texnologiyaning tez o‘zgarishi ishlab chiqarish jarayonini sekinlashtiradigan xavfsizlik talablarini e'tiborsiz qoldirishga olib kelishi mumkin. Har kuni yangi texnologiyalar joriy etilmoqda va tajovuzkorlar bir muncha vaqt o‘tgach, undan foydalanish uchun zaiflikni topadilar.

MUHOKAMA

Muvaffaqiyatli xavf tahlili uchun xavfsizlik bo‘yicha tahlilchi yangi texnologiyalar, mahsulotlar, tahdidlar yoki zaifliklar haqida ma'lumot olishi va almashishi va o‘zini xabardor qilishi kerak. Axborot tizimlariga tahdidlar aktivlarning maxfiyligi, yaxlitligi yoki mavjudligiga ta'sir qilishi mumkin. Tahdidlar yo‘q qilish (aktivni qayta tiklash mumkin emas), modifikatsiya qilish (aktivning ko‘rinishini o‘zgartirish), oshkor qilish (bilish zaruriyatini buzish) va xizmat ko‘rsatishdan bosh tortish kabi bir necha usulda harakat qilishi mumkin.

(resurslar vakolatli foydalanuvchilar uchun mavjud emas)

Axborot xavfsizligining umumiy tahdidlari quyida keltirilgan:

1. Inson xatosi yoki muvaffaqiyatsizligi (xodimlarning xatolari);
2. Mualliflik huquqini buzish;
3. Ruxsatsiz kirish yoki ma'lumotlarni yig'ish);
4. Axborotni qasddan tovlamachilik;
5. Qasddan qo‘poruvchilik harakatlari (tizimlar, ma'lumotlarni yo‘q qilish);
6. Uskunalar yoki ma'lumotlarni noqonuniy musodara qilish;
7. Qasddan dasturiy hujumlar (viruslar);
8. Tabiat kuchlari (yong'in, toshqin, zilzila, chaqmoq);
9. Xizmat ko‘rsatuvchi provayderlardan xizmat ko‘rsatish sifatining chetlanishi(elektr ta'minoti va global tarmoqqa texnik xizmat ko‘rsatish bilan bog'liq muammolar);
10. Texnik nosozliklar yoki uskunadagi xatolar (uskunalar ishdan chiqishi);
11. Texnik nosozliklar yoki dasturiy ta'minotdagi xatolar (xatolar, kod muammolari, noma'lum bo‘shliqlar);
12. Texnologik eskirish (eskirgan yoki eskirgan texnologiya).

XULOSA

Axborot xavfsizligi tashkilotning axborotiga ta'sir qiluvchi xavflarni kamaytirish maqsadida nazoratni ta'minlashga qaratilgan. Tanqidiy boshqa jiddiy tahdidlarni e'tiborsiz qoldirib, unchalik xavfli bo‘lmasligi mumkin bo‘lgan tavakkalchiliklarga pul sarflash xavfi mavjudligi muhim ahamiyatga ega. Xatarlarni boshqarish usullari tashkilotlarga tahdidlarni aniqlashga va ularni bartaraf etish uchun tejamkor xavfsizlik choralarini tanlashga yordam beradi. Va yo‘qotishlarning umumiy kutilayotgan narxini minimallashtirish.

ADABIYOTLAR RO‘YXATI (REFERENCES)

1. ISO/IEC 27005:2018. Information Technology—Security Techniques—Information Security Risk Management; ISO Standard: Geneva, Switzerland, 2018.

2. Kuzminykh, I.; Carlsson, A. Analysis of Assets for Threat Risk Model in Avatar-Oriented IoT Architecture. In Internet of Things, Smart Spaces, and Next Generation Networks and Systems; Galinina, O., Andreev, S., Balandin, S., Koucheryavy, Y., Eds.; Springer: Cham, Switzerland, 2018; Volume 11118, pp. 52–63.

Veb sayt

Williams, J. OWASP Risk Rating Methodology. OWASP. Available online:https://owasp.org/www-commu- nity/OWASP_Risk_Rating_Methodology (accessed on 11 January 2021).