GALAXY INTERNATIONAL FANLARARO TADQIQOT JURNALI (GIIRJ)
ISSN (E): 2347-6915
jild. 10, 9-son, sentabr (2022)

IQTISODIYOT SEKTORLARDAGI KIBER TAHDIQLAR, ZOJALIKLAR VA XAVFLAR

Ibragimov Nodirjon Nusriddinovich iffn
(PhD), TATU Qarshi filiali IT-servis
Kafedra dotsenti

Asqarova Nargiza Ilhomxo'jayevna TATU
Qarshi filiali IT kafedrasi assistenti

Amirov Akbarshoh Dilshod o'g'li TATU
Qarshi filiali IS-11-20 guruhi talabasi

Abdurahmonov Vohid Abdumuqim o'g'li
TATU Qarshi filiali IS-12-20 guruhi talabasi

ANTRACT

Kibertahdidlar, zaifliklar va xavflar kabi atamalar ko'pincha bir-birining o'rnida ishlatiladi va chalkashtiriladi. Ushbu maqola har bir atamani aniqlash, ular qanday farq qilishini ta'kidlash va bir-biri bilan qanday bog'liqligini ko'rsatishga qaratilgan.

Kalit so'zlar:DDoS, Phishing, SQL in'ektsiyalari, saytlararo skriptlar, xakerlar.

KIRISH

Kibertahdidlar yoki oddiygina tahdidlar kiberxavfsizlik holatlari yoki ularning oqibatlari tufayli zarar keltirishi mumkin bo'lgan hodisalarga ishora qiladi. Umumiy tahdidlarga bir nechta misollar: tajovuzkor troyan o'rnatishi va ilovalaringizdan shaxsiy ma'lumotlarni o'g'irlashiga olib keladigan ijtimoiy muhandislik yoki fishing hujumi, siyosiy faollar tomonidan veb-saytingizni DDoS o'g'irlashi, administratorning tasodifiy ma'lumotlarni tizimda himoyasiz qoldirishi. .

Kiberxavfsizlik tahdidlari tahdid qiluvchilar tomonidan amalga oshiriladi. Tahdid qiluvchilar odatda tahdidni boshlashi mumkin bo'lgan shaxslar yoki tashkilotlarga ishora qiladi. Tabiiy ofatlar, shuningdek, boshqa ekologik va siyosiy hodisalar xavf tug'dirsa-da, ular odatda tahdid sub'ektlari sifatida qaralmaydi. Umumiy tahdid sub'ektlariga misol qilib, moliyaviy sabablarga ko'ra jinoyatchilar (kiber jinoyatchilar), siyosiy motivli faollar (hacktivistlar) kiradi.),raqobatchilar, norozi xodimlar, norozi xodimlar va milliy davlat hujumchilari kiradi.

Agar tajovuzkorlar tizimga, jumladan, operatsion tizimga kirish uchun bir yoki bir nechta zaifliklardan foydalansa, kibertahdidlar yanada xavfli bo'lishi mumkin.

Zaifliklar shunchaki tizimdagi zaif tomonlarga ishora qiladi. Ular tahdidning natijasini mumkin va undan ham xavfli qiladi. Tizimdan bitta zaiflik orqali, masalan, bitta SQL Injection hujumi orqali foydalanish mumkin, bu tajovuzkorga nozik ma'lumotlar ustidan to'liq nazoratni berishi mumkin. Buzg'unchi ko'proq nazoratni qo'lga kiritish uchun bir nechta zaifliklardan foydalangan holda bir nechta ekspluatatsiyalarni birlashtirishi mumkin.

Umumiy zaifliklarga misollar: SQL Injections, Cross-sayt skriptlari, server noto'g'ri konfiguratsiyasi, oddiy matnda uzatiladigan nozik ma'lumotlar va boshqalar.

Xavflar ko'pincha tahdidlar bilan aralashtiriladi. Biroq, ikkalasi o'rtasida nozik farq bor. Kiberxavfsizlik xavfi tahdid ehtimoli va yo'qotish ta'sirining kombinatsiyasini anglatadi. Asosan, bu quyidagilarni anglatadi:

Shunday qilib, xavf bu stsenariy natijasida yuzaga kelishi mumkin bo'lgan yo'qotishlar bilan birga oldini olish kerak bo'lgan stsenariydir. Qanday qilib xavf yaratishingiz mumkinligi haqidagi faraziy misol:

1. SQL Injection - bu zaiflik.
2. Nozik ma'lumotlarni o'g'irlash SQL Injection imkon beradigan eng katta tahdidlardan biridir.
3. Moliyaviy maqsadli hujumchilar tahdidlardan biridir.
4. Maxfiy ma'lumotlarni o'g'irlash korxonalarga katta moliyaviy xarajatlarni (moliyaviy va obro'sini yo'qotish) olib keladi.
5. SQL Injection oson kirish mumkin bo'lgan, keng qo'llaniladigan zaiflik ekanligini va sayt tashqaridan ko'rilishini hisobga olsak, bunday hujum ehtimoli yuqori.

Shuning uchun, ushbu stsenariyda SQL Injection zaifligi yuqori xavfli zaiflik sifatida qaralishi kerak.

Zaiflik va kiber tahdid o'rtasidagi farq va zaiflik va xavf o'rtasidagi farqni tushunish odatda oson. Biroq, tahdid va xavf o'rtasidagi farq yanada nozik bo'lishi mumkin. Terminologiyadagi bu farqni tushunish xavfsizlik guruhlari va boshqa tomonlar o'rtasida aniqroq aloqa o'rnatish va tahdidlarning xavfga qanday ta'sir qilishini yaxshiroq tushunish imkonini beradi. Bu, o'z navbatida, xavfsizlik buzilishining oldini olish va yumshatishga yordam beradi. Xatarlarni samarali baholash va xavflarni boshqarish, tahdidlar ma'lumotlariga asoslangan samarali xavfsizlik echimlarini ishlab chiqish va samarali xavfsizlik siyosati va kiberxavfsizlik strategiyasini yaratish yaxshi tushunishni talab qiladi.

XULOSA

Xavfsizlik standartlarini ishlab chiqadigan mutaxassislar turli sohalarda qo'llaniladigan qoidalarni uyg'unlashtirishga ko'proq e'tibor berishlari kerak. Masalan, bir-birini to'ldirish tamoyillarida ko'rsatilgan yondashuvlardan foydalanish. Shuningdek, inson xatosi va tashkiliy zaifliklarni bartaraf etishni unutmang. Korxonalarda risklarni boshqarishni joriy etish xavfsizlik darajasini oshirishga yordam beradi.

ADABIYOTLAR RO'YXATI

1. Shubinskiy I.B. Strukturnaya nadyojnost axborot tizimi. Metody analiza /Ulyanovsk: Pechatnyy dvor, 2012.
2. BS 31100: 2008. Risklarni boshqarish - Amaliyot kodeksi.
3. BS OHSAS 18001:2007. Mehnatni muhofaza qilish va xavfsizlikni boshqarish tizimlari. Talablar.
4. CWA 15793: 2008. Laboratoriya biorisklarini boshqarish standarti.
5. ISO/IEC 51:1999. Xavfsizlik jihatlari - ularni standartlarga kiritish bo'yicha ko'rsatmalar.
6. ISO/IEC Guide 73:2009. Risklarni boshqarish - Lug'at - Standartlarda foydalanish bo'yicha ko'rsatmalar.
7. ISO 31000:2009. Risklarni boshqarish - printsiplar va ko'rsatmalar.
8. IEC/ISO 31010:2009. Risklarni boshqarish - Risklarni baholash usullari.
9. ISO 15190:2003. Tibbiy laboratoriyalar - xavfsizlik talablari.
10. Sabab J. Inson xatosi. - Nyu-York: Kembrij universiteti nashriyoti, 1990. -316 b.