ISSN 2181-3187

UNIVERSITET MAHALLIY KOMPYUTER TARMOQLARI UCHUN “MINOTAUR” XAVFSIZLIK TIZIMI

Xakimov Baxtiyorjon Baxromjon o‘g‘li
Furqat tuman kasb-hunar maktabi

Anatatsiya: Ushbu maqolada universitet mahalliy tarmoqlari uchun xavfsizlik tizimini yaratish uchun Minotaur loyihasi tasvirlangan. Loyihaning asosiy maqsadi ruxsatsiz kirish va boshqa tahdidlardan ishonchli himoyani ta'minlashdan iborat. Maqolada joriy tahdidlarni tahlil qilish, autentifikatsiya va avtorizatsiya mexanizmlarini ishlab chiqish va joriy etish, monitoring va tajovuzlarni aniqlash, ma'lumotlarni shifrlash va foydalanuvchilarni o'qitish masalalari mavjud. Loyihani ishlab chiqish bosqichlari va tizim ishtirokchilari o'rtasida rollarni taqsimlash ham taqdim etilgan. Taklif etilayotgan Minotaur tizimi zamonaviy tahdidlarga samarali qarshi turish va universitet tarmoqlarining barqaror ishlashini ta’minlash uchun kompleks yechim yaratishga qaratilgan

Kirish. Zamonaviy dunyoda ta'lim muassasalari axborot texnologiyalariga tobora ko'proq qaram bo'lib bormoqda. Universitet mahalliy tarmoqlari (LAN) o'qitish, o'rganish va tadqiqot uchun zarur bo'lgan resurslardan foydalanishni ta'minlash orqali ta'lim jarayonini qo'llab-quvvatlashda asosiy rol o'ynaydi. Bu ushbu tarmoqlarning xavfsizligini muhim qiladi. Ushbu maqolada universitetning mahalliy tarmoqlari uchun ruxsatsiz kirish va boshqa tahdidlarning oldini olishga qaratilgan “Minotavr” xavfsizlik tizimini yaratish loyihasi tasvirlangan.

Maqsad va vazifalar: Loyihaning asosiy maqsadi universitet mahalliy tarmoqlarini turli tahdidlardan samarali himoya qilishga qodir bo‘lgan kompleks xavfsizlik tizimini ishlab chiqish va joriy etishdan iborat. Ushbu maqsadga erishish uchun quyidagi vazifalar qo'yiladi:

1. Universitet tarmoqlaridagi mavjud tahdidlar va zaifliklarni tahlil qilish.
2. Foydalanuvchi autentifikatsiyasi va avtorizatsiya mexanizmlarini ishlab chiqish va joriy etish.
3. Monitoring va hujumlarni aniqlash tizimini joriy etish.
4. Maxfiy ma'lumotlarni himoya qilish uchun ma'lumotlarni shifrlash vositalarini joriy etish.
5. Foydalanuvchilarni axborot xavfsizligi asoslariga o‘rgatish.

Tahdid va zaiflik tahlili: Universitet tarmoqlari turli tahdidlarga duchor bo'ladi, jumladan:

1. Tarmoqqa ruxsatsiz kirish.
2. Zararli dastur.

ISSN 2181-3187

3. O'rtadagi odam hujumlari.
4. Fishing va ijtimoiy muhandislik.
5. Ma'lumotlar sizib chiqishi.

Ushbu tahdidlarga muvaffaqiyatli qarshi turish uchun zaifliklarni muntazam ravishda tahlil qilish va xavfsizlik tizimini yangi chaqiriqlarga muvofiq yangilash zarur.

Texnologiyalar va usullar:

Autentifikatsiya va avtorizatsiya

Tarmoqqa kirish xavfsizligini ta'minlash uchun ko'p faktorli autentifikatsiya (MFA) qo'llaniladi, u foydalanuvchi biladigan narsani (parol), ularda mavjud bo'lgan narsalarni (mobil qurilma) va ular (biometriya) birlashtiradi.

Monitoring va hujumni aniqlash

Buzilishlarni aniqlash va oldini olish tizimlarini (IDS/IPS) joriy etish real vaqtda shubhali faoliyatni aniqlash va hujumlarning oldini olish imkonini beradi. Ushbu tizimlar tarmoq trafigini tahlil qiladi va uni ma'lum tahdidlar ma'lumotlar bazasi bilan solishtiradi.

Ma'lumotlarni shifrlash

Maxfiy ma'lumotlarni himoya qilish uchun ma'lumotlarni shifrlash uzatish darajasida ham, saqlash darajasida ham qo'llaniladi. AES-256 va RSA kabi zamonaviy kriptografik algoritmlardan foydalaniladi.

Foydalanuvchilarni tayyorlash

Axborot xavfsizligi bo'yicha muntazam treninglar va seminarlar foydalanuvchilarga ehtimoliy tahdidlarni tushunishga va ularga to'g'ri javob berishga yordam beradi.

Loyihani ishlab chiqish bosqichlari:

Minotaur xavfsizlik tizimi loyihasi bir necha asosiy bosqichlardan o'tmoqda. Ularning har biri umumiy maqsadga erishishga qaratilgan aniq vazifalar va tadbirlarni o'z ichiga oladi.

1-bosqich: Tahlil va rejalashtirish

Ushbu bosqichda mavjud infratuzilmaning batafsil tahlili va potentsial tahdidlar va zaifliklarni aniqlash amalga oshiriladi. Asosiy vazifalarga quyidagilar kiradi:

1. Universitet tarmog'i xavfsizligining hozirgi holatini baholash.
2. Potentsial tahdidlar to'g'risida ma'lumotlarni to'plash va tahlil qilish.
3. Xavfsizlik tizimi talablarini aniqlash.
4. Belgilangan muddatlar va resurslarni ko'rsatadigan loyiha rejasini ishlab chiqish.

2-bosqich: tizim dizayni

Dizayn bosqichida barcha kerakli komponentlar va ularning o'zaro ta'sirini o'z ichiga olgan xavfsizlik tizimi arxitekturasi ishlab chiqiladi. Asosiy maqsadlar:

ISSN 2181-3187

• Tahdid va xavf modelini yaratish.

• Tizim arxitekturasini ishlab chiqish, jumladan autentifikatsiya, avtorizatsiya, shifrlash, monitoring va foydalanuvchilarni o'qitish.

• Uskunalar va dasturiy ta'minot uchun texnik talablarni aniqlash.

• Loyiha hujjatlarini tayyorlash.

3-bosqich: ishlab chiqish va amalga oshirish

Rivojlanish bosqichi barcha xavfsizlik tizimining tarkibiy qismlarini yaratish va birlashtirishni o'z ichiga oladi. Asosiy maqsadlar:

• Autentifikatsiya va avtorizatsiya uchun dasturiy ta'minotni ishlab chiqish.

• Monitoring va hujumlarni aniqlash uchun IDS/IPS tizimlarini joriy etish.

• Ma'lumotlarni shifrlash vositalarini sozlash.

• Foydalanuvchilar uchun o'quv dasturlarini ishlab chiqish va amalga oshirish.

• Barcha komponentlarni yagona tizimga integratsiyalash va sinov stendlarida sinovdan o'tkazish.

4-bosqich: Sinov va optimallashtirish

Ushbu bosqichda kamchiliklarni aniqlash va bartaraf etish uchun xavfsizlik tizimining kompleks sinovlari o'tkaziladi. Asosiy maqsadlar:

• Funktsional va yuk sinovlarini o'tkazish.

• Xatolar va zaifliklarni aniqlash va tuzatish.

• Tizim ish faoliyatini optimallashtirish.

• Hujumlarga chidamliligini tekshirish uchun penetratsion testlarni o'tkazish.

5-bosqich: Amalga oshirish va texnik xizmat ko'rsatish

Muvaffaqiyatli sinovdan so'ng tizim ishga tushiriladi va qo'llab-quvvatlanadi. Asosiy maqsadlar:

• Universitet tarmog'ining qismlaridan birida tizimni sinovdan o'tkazish.

• Sinovni amalga oshirish natijalarini baholash va zarur tuzatishlar kiritish.

• Universitetning barcha kafedralarida tizimni keng miqyosda joriy etish.

• Xavfsizlik tizimining muntazam yangilanishi va uning ishlashini nazorat qilish.

• Foydalanuvchilarni qo'llab-quvvatlash va qo'llab-quvvatlash.

6-bosqich: Keng miqyosda amalga oshirish va texnik xizmat ko'rsatish

Muvaffaqiyatli sinovdan so'ng va zarur tuzatishlar kiritilgach, tizim universitetning barcha bo'limlarida joriy etilmoqda. Asosiy maqsadlar:

• Universitetning barcha kafedralarida tizimni keng miqyosda joriy etish.

• Xavfsizlik tizimining muntazam yangilanishi va uning ishlashini nazorat qilish.

• Foydalanuvchilarni qo'llab-quvvatlash va qo'llab-quvvatlash.

7-bosqich: Baholash va takomillashtirish

Yakuniy bosqichda joriy etilgan xavfsizlik tizimining samaradorligi baholanadi va kelgusida takomillashtirish rejalashtirilgan. Asosiy maqsadlar:

• Tizimning ishlashi bo'yicha ma'lumotlarni to'plash va tahlil qilish.

ISSN 2181-3187

- Tizimning belgilangan maqsadlar va talablarga muvofiqligini baholash.
- Tizimni takomillashtirish bo'yicha tavsiyalar ishlab chiqish.
- Kelajakdagi yangilanishlar va yangilanishlarni rejalashtirish.

Xavfsizlik tizimidagi rollar:

Minotaur xavfsizlik tizimining samarali ishlashi uchun barcha ishtirokchilarning roli va mas'uliyati aniq belgilanishi kerak. Bu yuqori darajadagi himoyani ta'minlashga va har qanday tahdidlarga tezda javob berishga yordam beradi. Asosiy rollarga quyidagilar kiradi:

1. Tarmoq administratori

Tarmoq ma'muri Universitet tarmog'ini boshqarish va xavfsizligini ta'minlash uchun asosiy mas'uliyatga ega. Uning mas'uliyatiga quyidagilar kiradi:

- Xavfsizlik apparati va dasturiy ta'minotini sozlash va boshqarish.
- Tarmoq trafigini kuzatib boring va potentsial tahdidlarni aniqlang.
- Foydalanuvchiga kirishni boshqarish va kirish huquqlarini boshqarish.
- Yangi zaifliklardan himoya qilish uchun tizimlarni yangilash va tuzatish.
- Xavfsizlik tekshiruvlari va kirish testlarini o'tkazish.
- Xodimlar va foydalanuvchilarni axborot xavfsizligi asoslariga o‘rgatish.

2. Foydalanuvchilar

Tarmoq foydalanuvchilariga universitet talabalari, professor-o‘qituvchilari va xodimlari kiradi. Ularning asosiy mas'uliyati xavfsizlik qoidalari va siyosatlariga rioya qilishdir. Ularning majburiyatlariga quyidagilar kiradi:

- Murakkab parollardan foydalaning va ularni muntazam ravishda o'zgartiring.
- Tarmoq resurslariga kirishda xavfsizlik siyosatiga rioya qilish.
- Shubhali harakat yoki hodisalar haqida administratorni xabardor qilish.
- Axborot xavfsizligi bo'yicha o'quv dasturlarida ishtirok etish.

3. Axborot xavfsizligi bo'yicha mutaxassislar

Axborot xavfsizligi bo'yicha mutaxassislar xavfsizlik strategiyalari va boshqaruvlarini ishlab chiqish va amalga oshirish uchun mas'uldirlar. Ularning vazifalariga quyidagilar kiradi:

- Tahdidlar va zaifliklarni tahlil qilish va ularga qarshi choralar ishlab chiqish.
- Xavfsizlik siyosati va protseduralarini ishlab chiqish.
- Foydalanuvchilar va ma'murlar uchun treninglar va seminarlar o'tkazish.
- Xavfsizlik tizimini tekshirish va baholash.

4. Universitet boshqaruvi

Universitet rahbariyati xavfsizlik tizimini saqlash va moliyalashtirishda asosiy rol o'ynaydi. Ularning majburiyatlariga quyidagilar kiradi:

- Axborot xavfsizligi sohasida ustuvorlik va maqsadlarni aniqlash.
- Xavfsizlik choralarini amalga oshirish uchun resurslarni ta'minlash.
- Xavfsizlik siyosatini tasdiqlash va ularning bajarilishini nazorat qilish.

ISSN 2181-3187

• Xavfsizlik darajasini oshirish tashabbuslarini qo'llab-quvvatlash.

5. Tarmoq uskunalari muhandislari

Tarmoq muhandislari tarmoq qurilmalarini o'rnatish, sozlash va saqlash uchun javobgardir. Ularning vazifalariga quyidagilar kiradi:

• Routerlar, kalitlar va kirish nuqtalari kabi uskunalarni o'rnatish va sozlash.

• Tarmoq qurilmalarining dasturiy ta'minotini qo'llab-quvvatlash va yangilash.

• Tarmoq uskunasidagi nosozliklarni bartaraf etish.

• Tarmoq qurilmalarining jismoniy xavfsizligini ta'minlash.

6. Dasturiy ta'minot muhandislari

Dasturiy ta'minot muhandislari xavfsizlik dasturiy ta'minoti komponentlarini ishlab chiqadilar va qo'llab-quvvatlaydilar. Ularning majburiyatlariga quyidagilar kiradi:

• Autentifikatsiya, monitoring va kirishni boshqarish uchun dasturiy ta'minotni ishlab chiqish va sinovdan o'tkazish.

• Dasturiy ta'minotni mavjud tizimlar va infratuzilma bilan integratsiyalash.

• Zaifliklarni bartaraf etish uchun dasturiy ta'minotni yangilash va tuzatish.

• Foydalanuvchini qo'llab-quvvatlash va muammolarni hal qilish.

Xulosa:

Universitet lokal tarmoqlari uchun “Minotavr” xavfsizlik tizimini yaratish va joriy etish ta’lim muassasalarining axborot resurslarini himoya qilish yo‘lidagi muhim qadamdir. Bizning loyihamiz zamonaviy tahdidlarga samarali qarshi turadigan va universitet tarmoqlarining xavfsiz va ishonchli ishlashini ta'minlaydigan kompleks yechim yaratishga qaratilgan. Kelgusida taklif etilayotgan tizimni sinovdan o‘tkazish va real ma’lumotlar asosida samaradorligini keyinchalik baholash rejalashtirilgan.

Adabiyotlar ro'yxati:

1. Vendrov, A. M., Ivkin, V. V. Kompyuter tizimlarining xavfsizligi: darslik. M .: "Piter" nashriyoti, 2013. 400 b.
2. Lukatkin, V. I., Lukatkin, S. V. Axborot xavfsizligi: darslik. M.: Yurait, 2018. 256 b.
3. Kostina, I. S., Kostin, A. A. Axborot xavfsizligini tashkil etish: universitetlar uchun darslik. M.: Yurayt nashriyoti, 2015. 336 b.
4. Shniperman, F.A. Axborot xavfsizligi. Kurs ishi uchun uslubiy ko'rsatmalar va topshiriqlar. M.: Yurayt nashriyoti, 2018. 84 b.
5. Volkov, V.V., Zuev, V.S. Axborot xavfsizligi asoslari: darslik. Sankt-Peterburg: Politexnika universiteti nashriyoti, 2016. 272 p.
6. Axborot xavfsizligi tushunchalari [Elektron resurs]: darslik / komp. S. A. Gusarov, O. V. Lobanova. M.: "Imtihon" nashriyoti, 2007. 334 b. URL: https://e.lanbook.com/book/3002086.

ISSN 2181-3187

7. Gordienko, E. I. Axborot xavfsizligi tizimlari: universitetlar uchun darslik. M.: Flinta, 2019. 312 b.
8. Mironov, V.V., Makarov, V.V. Axborot xavfsizligi. M.: Flinta, Nauka, 2019. 240 b.
9. Romanenko, O.V. Axborot xavfsizligi. “Informatika va informatika” fanidan talabalar uchun kurs ishini bajarish bo‘yicha uslubiy ko‘rsatmalar. M.: "Infra-M" nashriyoti, 2018. 58 b.
10. Martynov, A. A. Axborot xavfsizligi va axborotni himoya qilish: darslik. M.: Yurayt nashriyoti, 2014. 320 b.
11. Leontiev, A. A., Solodushkin, S. Yu. Ma'lumotlar uzatish tarmoqlarida xavfsizlik: darslik. M.: Yurayt nashriyoti, 2014. 308 b.