METHODS AND TOOLS FOR DETECTING ATTACK TRACES IN INFORMATION SYSTEMS

Jo'rayeva Yodgora Suyun Qizi
Tashkent University of Information Technologies named after
Muhammad Al-Khwarizmi , Faculty of "Information Security", 1st year master of Information Security direction

Annotation. The article analyzes modern methods of detecting attacks in order to identify shortcomings in the practical application of information systems, the methods and algorithms used, as well as existing software and hardware tools for detecting these attacks.

Keywords: Information systems, new generation firewalls, security tracking systems, traffic analysis systems, endpoint detection.

So'nggi 30 yil ichida zararli faoliyatni aniqlash usullari keskin yaxshilandi. Agar ilgari xakerlar yollangan informatorlar orqali ushlangan bo'lsa, endi kelishuv izlarini qidirish aqlli aniqlash va avtomatlashtirilgan tahlil yordamida amalga oshiriladi. Zararli dasturiy ta'minot kampaniyalarining dastlabki kunlarida imzolardan foydalangan antivirus yechimlari (virus kodlari namunalari) zararli dasturlarni aniqlashga yordam berdi. Keyin virusga qarshi himoya qilishda yanada aqlli texnologiyalar paydo bo'ladi - evristik aniqlash va xulq-atvorni tahlil qilish.

Antivirus vositalarini ishlab chiqishni misol tariqasida, tarmoq trafigi va turli xil IT tizimlarining raqamli hodisalarida anomaliyalarga asoslangan kompyuter hujumlarini aniqlashning boshqa usullari haqida ham aytish mumkin. Ma'lumotlarni qayta ishlash va ulardan foydalanishning yangi texnologiyalari, shuningdek, biznes jarayonlarini avtomatlashtirish vositalari yaratilishi bilan yangi tahdidlar paydo bo'lmoqda. Hujumchilarning texnikasi va taktikasini ishlab chiqish, yangi tahdidlar va zaifliklarning paydo bo'lishi axborot infratuzilmalarining turli darajalarida: jismoniydan amaliygacha qo'llaniladigan kompyuter hujumlarini aniqlash texnologiyalari rivojlanishining asosiy omilidir. Shu bilan birga, texnologiyalar kompyuter hujumlari faktidan keyin paydo bo'lishini aytadi.

Hozirgi vaqtda turli xil dasturiy ta'minot ishlab chiqaruvchilari tomonidan kompyuter hujumlarini aniqlash texnologiyalari faol ravishda ishlab chiqilmoqda. Dasturiy ta'minot ishlab chiqaruvchilari o'z mahsulotlariga kiritadigan asosiy vositalar - axborot tizimidagi o'zgarishlarni kuzatish, aniqlash va tahlil qilish. Yechimlar murakkablashmoqda va turli xil vositalarni birlashtiradi.

Ba'zi tashkilotlarda faqat asosiy himoya vositalari qo'llaniladi, bu esa, aksariyat, hollarda murakkab maqsadli hujumlarni o'z vaqtida aniqlash va sodir bo'lgan voqealarni to'liq tahlil qilish uchun yetarli emas.

Yaqinda paydo bo'lgan detektorlarning sinflarini ko'rib chiqamiz.

1) Keyingi avlod xavfsizlik devorlari (NGFW)

Amaliyot printsipi, asosan, paketli filtrlash va tarmoq ulanishlarini boshqarishda bo'lgan an'anaviy xavfsizlik devorlari yangi avlod yechimlari bilan almashtirildi. Yechimlar sinfi uzoq vaqt oldin paydo bo'lgan, ammo uni zamonaviy aniqlash texnologiyalari to'plamida ko'rib chiqishga arziydi. Keyingi avlod xavfsizlik devorlari klassik xavfsizlik devori va NGFW-da turli xil kombinatsiyalarda ishlatilishi mumkin bo'lgan zamonaviy texnologiyalarning funktsiyalarini birlashtiradi:

- Application Layer Firewall (WAF) funktsiyalari;
- Xavfni aniqlash va blokirovka qilish uchun imzo trafigini tahlil qilish (IPS);
- Har xil darajadagi protokollar bilan shifrlangan trafikni to'liq matnli tahlil qilish (tekshirish);
- Trafikni cheklash va birinchi o'ringa qo'yish qobiliyati - Xizmat ko'rsatish sifati (QoS);
- Xavfsiz holatdagi fayllarni xulq-atvori tahlili (qum qutilari);

• Dolzarb tahdidlar to'g'risidagi ma'lumotlar bilan doimiy ravishda boyitish (obro'-e'tibor ro'yxatlari, murosaga erishish ko'rsatkichlari va boshqalar)

Bundan tashqari, NGFW ishlab chiqaruvchisi va konfiguratsiyasiga qarab DNS hujumlaridan himoya qilish, josuslarga qarshi dasturlardan himoya qilish (ruxsatsiz ma'lumot to'plash yoki sozlamalarni o'zgartirish uchun shpion dasturlari), botnetlarga ulanishlarni boshqarish va boshqa qo'shimcha funktsiyalarni o'z ichiga olishi mumkin.

Xulosa qilib aytganda, NGFW - bu dastur qatlami trafigini boshqarish, ichki kirishni aniqlash tizimi va trafikni foydalanuvchi identifikatoriga ega bo'lgan qurilma. Amalda, masalan, fishing xabarlarini aniqlash va undan himoya qilishning bir qismi sifatida NGFW elektron pochta qutilariga kelgan veb-havolalarni tekshiradi va agar ular zararli manbalarga olib keladigan bo'lsa, ularni bloklaydi. Tekshirish obro'-e'tibor ro'yxatlari va murosaga erishish ko'rsatkichlari ma'lumotlar bazalariga muvofiq amalga oshiriladi. Bundan tashqari, keyingi avlod xavfsizlik devorlari elektron pochta va elektron pochta qo'shimchalarini tahlil qilishi va zararli kod bo'lsa, ularni bloklashi mumkin. NGFW qurilmalari yordamida hujumlarni aniqlashning ko'plab ssenariylari mavjud.

Xavfsizlikni kuzatish tizimlari (SIEM)

Xavfsizlik haqida ma'lumot va tadbirlarni boshqarish (SIEM) yechimlari turli xil axborot tizimlari va ilovalaridagi voqealarni kuzatish uchun mo'ljallangan. Ushbu sinfning axborot xavfsizligi yechimlari quyidagi vazifalarni bajarishga imkon beradi:

• xavfsizlik bo'yicha katta hajmdagi tadbirlarni yig'ish va tahlil qilish;
• IT infratuzilmasini himoya qilish vositalarining hozirgi holatini monitoring qilish;
• real vaqtda kompyuter hodisalarini aniqlash;
• IT infratuzilmasida sodir bo'layotgan narsalar to'g'risida to'liq tasavvurga ega bo'lish;
• AT va axborot xavfsizligi tizimlari ishidagi xatolarni aniqlash va ularga javob berish;
• hujum zanjirlarini bashorat qilish uchun tarmoq xaritasini yaratish;
• real vaqtda tahlil qilish va xavfni baholash uchun ma'lumot olish;
• qonunchilikning ayrim talablari va normativ hujjatlarini bajarish

Ko'pincha tajovuzkorlar infratuzilma ichiga kirib, o'z o'rnini egallaydi va shu bilan birga uzoq vaqt davomida sezilmasdan qoladi. Bunday kirib borishdan maqsad ma'murlar va axborot xavfsizligi bo'yicha mutaxassislar uchun ko'rinmaydigan ma'lumotlarni buzish yoki ichkaridan muhim infratuzilma tugunlariga hujumlarni tayyorlash va tashkil etishdir. Voqealarni yanada samarali aniqlash va maqsadli tizimga bunday kirib borishga qarshi kurashish uchun SIEM yechimlari tahdidlar (yangiliklar, kelishuv ko'rsatkichlari, ekspertlarning o'zaro bog'liqligi qoidalari va boshqalar) haqidagi eng dolzarb ma'lumotlardan foydalangan holda voqealarni retrospektiv tahlil qilishga imkon berishi muhimdir.

SIEM sinfi yechimlarining ishlash prinsipi dasturiy ta'minot darajasida ham, apparat komponentlari darajasida ham turli xil qurilmalardan har xil jurnallarni (hodisalarni) yig'ishdir. Bundan tashqari, barcha voqealar keyingi tahlil qilish uchun yagona formatga tushiriladi. Xuddi shu infratuzilma elementi bilan bog'liq bo'lgan hodisalar to'plami (korrelyatsiya) kiberhujumni ko'rsatishi mumkin.

SIEM sizga AT infratuzilmasida sodir bo'layotgan voqealar to'g'risida to'liqroq tasavvurga ega bo'lishga va qo'shimcha ravishda ma'lum tugunlarning tarmoqqa ulanish imkoniyatlarini tahlil qilishga imkon beradi.

Turli xil manbalardan olingan ma'lumotlarni diqqat bilan tahlil qilish va o'zaro bog'lash orqali SIEM alohida ishlaydigan an'anaviy aniqlash vositalari har doim ham samarali bo'lmaydigan hodisalarni aniqlaydi.

Odatda SIEM foydalanish holatlari:

• Axborot tizimlari elementlarini yuqtirish holatlarini kuzatish, veb-proksi jurnallari, ichki ulanish jurnallari va boshqalarni ishlatadigan zararli dasturlarni (zararli dasturlarni) aniqlash;
• ichki tizimdagi tizim o'zgarishi va boshqa ma'muriy harakatlarni va ularning ruxsat etilgan siyosatlarga muvofiqligini kuzatib borish;
• autentifikatsiya, shuningdek, foydalanuvchi akkauntlari buzilishining monitoringi;
• IS siyosatiga muvofiqligini nazorat qilish.

Trafikni tahlil qilish tizimlari (NTA)

Network Traffic Analysis (NTA) yechimlari tarmoq hujumlarini aniqlash, tarmoq trafigini ushlab turish va tahlil qilish uchun mo'ljallangan. Ushbu tizim hujumning dastlabki bosqichida tajovuzkorlar mavjudligini aniqlash, tahdidlarni tezda lokalizatsiya qilish, shuningdek, axborot xavfsizligi qoidalariga rioya qilishni ta'minlashga yordam beradi.

Standart tarmoq analizatorlaridan (IDS / IPS) farqli o'laroq, NTA tizimlari nafaqat perimetrda, balki AT infratuzilmasida ham trafikni tahlil qiladi.

Ushbu yechimlar sinfi dalil bazasini shakllantirish uchun tarmoq trafigi seanslarini tejash va uni huquqni muhofaza qilish idoralariga va axborot resurslariga kompyuter hujumlarini aniqlash, oldini olish va yo'q qilish davlat tizimiga o'tkazish qobiliyatiga ega. Bundan tashqari, zamonaviy imzolarning paydo bo'lishi bilan NTA sinfidagi yechimlar arxivda saqlanadigan tarmoq trafigini tahlil qilish imkoniyatiga ega bo'lishi kerak (retrospektiv tahlil).

NTA sinfidagi yechimlar murakkab maqsadli hujumlar aniqlangan vaziyatlarda SIEM sinf yechimlari uchun tarmoq voqealarining qo'shimcha manbai bo'lishi mumkin.

Amalda bunday yechimlar, masalan, ruxsatsiz xostdan domen boshqaruvchisiga ulanish uchun shubhali urinishni aniqlashga imkon beradi, so'ngra xostning tarmoq faoliyati to'g'risidagi tarixiy ma'lumotlarni tahlil qiladi va shunga o'xshash boshqa urinishlar mavjudligini tekshiradi. Agar ular sodir bo'lgan bo'lsa, unda bu maqsadli hujum yoki hech bo'lmaganda xakerlik urinishlari haqida gapiradi.

Oxirgi nuqta hujumini aniqlash (EDR)

Endpoint Detection and Response (EDR) yechimlari so'nggi qurilmalarga kompyuter hujumlarini aniqlashga imkon beradi va axborot xavfsizligi bo'yicha mutaxassislarning javoblari uchun zarur ko'rsatkichlarni beradi.

Ushbu yechimlar sinfi odatda so'nggi qurilmaga o'rnatilgan maxsus agentdan foydalanadi. Uning funktsiyalari foydalanuvchilar va dasturiy ta'minot faoliyati to'g'risidagi ma'lumotlarni to'plash, murosaga kelish belgilarini aniqlash (murosaga kelish ko'rsatkichlari), buzilgan moslamalarni aniqlash va lokalizatsiya qilishda yordam berish va boshqalarni o'z ichiga oladi. Barcha to'plangan ma'lumotlar kompyuterdagi hodisalarni tekshirishda yordam beradi.

Amalga oshirilishiga qarab, EDR yechimi turli xil aniqlash texnologiyalarini o'z ichiga olishi mumkin. Masalan, ma'lumotlarni yig'ish va tahlil qilish agentidan tashqari, bu xatti-harakatlarni tahlil qilish, murosaga kelish ko'rsatkichlarini tahlil qilish, shuningdek tahdid ma'lumotlarini boyitish uchun SIEM tizimlari va Threat Intelligence tizimlari bilan avtomatik o'zaro aloqada antivirusdan himoya qilish vositasi bo'lishi mumkin. Axborot xavfsizligi bo'yicha mutaxassislarga yuqori sifatli tekshiruv o'tkazish uchun nima bo'lganligi to'g'risida to'liqroq ma'lumot beradi.

EDR yechimlari tashkilotlarga an'anaviy so'nggi mudofaani chetlab o'tishga qaratilgan murakkab tahdidlarni aniqlashga imkon beradi.

NDR yechimlari tahdidni real vaqtda aniqlash bilan to'liq tarmoq ko'rinishini ta'minlaydi, EDR va SIEM mahsulotlari bilan integratsiya esa hodisalarni aniqlash uchun qo'shimcha, aniqroq ma'lumotlar korrelyatsiyasini ta'minlaydi.

Kompyuter tahdidlarini hisobga olish va qayta ishlash tizimlari (Threat Intelligence)

Threat Intelligence yechimlari AT infratuzilmasidagi zaifliklar va tahdidlar bo'yicha zamonaviy tahlillarni amalga oshirishga imkon beradi. Tahlil tahdid to'g'risidagi ma'lumot yoki tahdidga oid razvedka ma'lumotlari (TIF) asosida amalga oshiriladi.

Threat Intelligence Platform - tahdid ma'lumotlarini boyitish, aniqlash, tarqatish va o'zaro bog'lash uchun ixtisoslashgan platformadir. Ushbu yechimlar sinfi avtomatik ravishda lentalarni bog'lashga, ularni kontekstli ma'lumotlar bilan to'ldirishga imkon beradi. TI platformalarining afzalligi - bu siz uchun mavjud bo'lgan tahdidlar to'g'risidagi har qanday ma'lumot manbalarini birlashtirish va markazlashtirilgan tarzda qayta

ishlash, shuningdek, uni boshqa kiberxavfsizlik vositalari bilan, masalan, SIEM tizimlari, hodisalarga javob berish platformalari yoki himoya vositalari bilan birlashtirish qobiliyatidir.

Xakerlar uchun aldovlar **(«Honeypot»)**

Honeypot yechimlari sinfi xakerlik hujumlarini aniqlash va hujumlarni bashorat qilish va qarshi choralarni ko'rish usullarini o'rganish uchun mo'ljallangan. Maxsus ochiq portlari, zaifliklari va boshqa aniq kamchiliklari bo'lgan sanoat tizimlaridan ajratilgan muhit "aldanish" sifatida ishlatiladi. Maqsadlar veb-server, virtual mashina, tarmoq qurilmasi va boshqa tizimlar va xizmatlar bo'lishi mumkin. Hujumchilarni aniqlash uchun mo'ljallangan muhit ichida kiberjinoyatchilarda qiziqish uyg'otish uchun turli xil manbalarni muhim fayllar, pochta xabarlari, hisob ma'lumotlari sifatida yashirish mumkin.

Bundan tashqari, fishingga qarshi kurashish uchun veb-sayt kodiga kiritilgan honeypot havolalari ishlatiladi, bu esa veb-saytni klonlash holatlarini aniqlashga imkon beradi va himoyachilarga mumkin bo'lgan hujum haqida ogohlantiradi.

Texnologiya rivojlanishda davom etmoqda va turli xil vositalar nafaqat ishlatilgan usullarni, balki tajovuzkorlar o'z tizimlariga ulanganidan keyin, masalan, terminal oynasida yozib olishdan keyin ularning harakatlarini ham ochib beradigan ko'rinadi. Bu sizga tajovuzkorlarning o'zlari haqida ko'proq ma'lumot olish va ular qanday boshqa tizimlarga ulanganligini aniqlash imkonini beradi.

Xulosa qilib aytadigan bo’lsak, ko'pgina tashkilotlar kutilgan hujumlarning qisqa ro'yxati asosida infratuzilma hujumlarini aniqlash tartiblarini tizimlashtirdilar. Biroq, tahdid manzarasi shu qadar tez sur'atlar bilan rivojlanadiki, ko'plab aniqlash jarayonlari tezda eskirmoqda.

IT texnologiyalarining rivojlanishi bilan kiber kosmosda yangi tahdidlar paydo bo'lmoqda. Hujumchilar o'z vositalarini takomillashtirmoqdalar va maqsadlariga erishish uchun tobora murakkab usullarni topmoqdalar.

Hujumlarni dastlabki bosqichda aniqlash uchun zararli faoliyatni tahlil qilish va aniqlash, shuningdek, mumkin bo'lgan ruxsatsiz ta'sirni bashorat qilish uchun har xil texnologiyalarni har tomonlama tatbiq etadigan eng zamonaviy aniqlash vositalaridan foydalanish kerak. Shu bilan birga, muvaffaqiyatli hujum paytida (sezgir ma'lumotlarning yo'qolishi, moliyaviy zarar va h.k) axborot tizimlari faoliyatidagi buzilish oqibatlarini va joriy etilayotgan texnologiyalarni aniqlash narxlarini taqqoslash juda muhimdir. Minimal talab qilinadigan yechimlar to'plamini tanlashda sohaning o'ziga xos xususiyatlari, foydalaniladigan texnologiyalar, kiberxavfsizlikning mavjud tahdidlari va xatarlari, shuningdek xavfsizlik darajasidagi qonun talablari hisobga olinishi kerak.

Aniqlash vositalarini tanlashga mutanosib yondashuvni qo'llash, axborot xavfsizligini boshqarish tizimini yanada samarali tashkil etishga imkon beradi va kompyuter hujumi sodir bo'lgan taqdirda katta (qabul qilinmaydigan) zararni oldini oladi.

Foydalanilgan adabiyotlar ro’yxati

1. Сергей Куц “Технологии обнаружения компьютерных атак” https://safe-surf.ru/specialists/article/5274/656701/
2. Селин Р. Н. «Программная система и способ выявления угроз информационной безопасности в компьютерных сетях» Автореферат диссертации на соискание ученой степени кандидата технических наук. г: Ростов-на-Дону-2011
3. Селин Р.Н. О методах защиты информации в базах данных Oracle [Текст] / Селин Р.Н., Хади Р.А. // Материалы IV международной научно-практической конференции "Методы и алгоритмы прикладной математики в технике, медицине и экономике", Юж.-Рос. гос. техн. ун-т (НПИ). Новочеркасск: ЮРГТУ, 2004.
4. Селин Р.Н. Метод поиска многих образцов с ошибками [Текст] / Селин Р.Н., Аграновский А.В., Гуфан К.Ю. // Научно-технический журнал "Системы управления и информационные технологии", №4.1(26), 2006