Також в базі представлені 22 типи атак. При цьому атаки поділяються на 4 основні категорії: DoS, U2R, R2L і Probe.

DoS атаки - це мережеві атаки, спрямовані на виникнення ситуації, коли на системі, що є атакованою, відбувається відмова в обслуговуванні. Дані атаки характеризуються генерацією великого обсягу трафіку, що призводить до перевантаження і блокування сервера. Виділяють шість DoS атак: back, land, neptune, pod, smurf, teardrop.

U2R атаки передбачають отримання зареєстрованим користувачем привілеїв локального суперкористувача (мережевого адміністратора). Виділяють чотири типи U2R атак: buffer_overflow, loadmodule, perl, rootkit.

R2L атаки характеризуються отриманням доступу незареєстрованого користувача до комп'ютера з боку віддаленого комп'ютера. Виділяють вісім типів R2L атак: ftp_write, guess_passwd, imap, multihop, phf, spy, warezclient, warezmaster.

Probe атаки полягають в скануванні мережевих портів з метою отримання конфіденційної інформації. Виділяють чотири типи Probe атак: ipsweep, nmap, portsweep, satan [2].

Зовнішній вигляд бази KDD99 – текстовий файл у якому у вигляді матриць представлено набір параметрів певного типу атаки або нормального з'єднання.

```
0,tcp,http,SF,215,45076,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,1,1,0.
00,0.00,0.00,0.00,1.00,0.00,0.00,0,0,0.00,0.00,0.00,0.00,0.00,
0.00,0.00,0.00,normal.
0,tcp,http,SF,162,4528,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,2,2,0.0
0,0.00,0.00,0.00,1.00,0.00,0.00,1,1,1.00,0.00,1.00,0.00,0.00,0
.00,0.00,0.00,normal.
```

Рисунок 1 – Зовнішній вигляд бази NSL-KDD

Переваги:

1. Не включає надлишкових записів в набір ознак.
2. У запропонованих тестових наборах не містить дублікатів записів.
3. Кількість відібраних записів з кожної складної групи є обратно пропорційною відсотковій кількості записів у вихідному наборі даних KDD. Як результат, класифікаційні показники різних методів машинного навчання змінюються в більш широкому діапазоні, що робить більш ефективним точне оцінювання різних методів навчання.

Недоліки:

1. Досить велика кількість параметрів, що знижує час виявлення вторгнень. Тому на практиці використовують не всі.

Список використаних джерел

1. KDD Cup 1999 Data [Електронний ресурс] – Режим доступу до ресурсу: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html.
2. Марков Р. А., Бухтояров В. В., Попов А. М., Бухтоярова Н. А. Дослідження нейромережевих технологій для виявлення інцидентів інформаційної безпеки // Молодий вчений. - 2015. - №23. - С. 55-60. - URL https://moluch.ru/archive/103/23866/
3. DERIVED FEATURES [Електронний ресурс] – Режим доступу до ресурсу: http://kdd.ics.uci.edu/databases/kddcup99/task.html

---

УДК 004.457

UBA/UEBA - СИСТЕМИ

Гринько В.В., студ. гр. КБ-171, **Мехед Д.Б.,** к.п.н., доцент кафедри
кібербезпеки та математичного моделювання
Чернігівський національний технологічний університет

Сьогодні дуже важливим чинником належного функціонування підприємств та компаній є високий рівень інформаційної безпеки. Інформаційна безпека означає безпеку всієї інформаційної середовища: це значить, що під захистом повинні знаходитися не тільки самі дані, але і їх носії, а також вся інфраструктура. Рішення для забезпечення ІБ повинні охоплювати технічні, адміністративні, правові аспекти, а також поведінку користувача, щоб не допустити витоків і розголошення комерційної таємниці. Цільових атак стало більше, вони стали більш витонченішими і більш продуманими, зловмисники стали хитрішими та розумнішими, а кількість інформаційних систем збільшилась. В такому світі контролювати і реагувати на інциденти інформаційної безпеки стає все складніше і дорожче. Тому перед індустрією інформаційної безпеки стоїть велика кількість завдань по автоматизації процесів реагування на інциденти і загрози та їх виявлення. Одне з цих завдань вирішують системи UBA/UEBA..

UBA – система є одним з основних інструментом захисту ІБ. UBA - система, що дозволяє на основі даних про користувачів з допомогою алгоритмів машинного навчання і аналізу будувати моделі поведінки користувачів і визначати відхилення від цих моделей, тобто ця система використовує технології

машинного навчання і обробки даних для того, щоб виявити аномальну активність користувачів корпоративної інформаційної системи.[1]

Щоб зрозуміти, для чого потрібна UBA – система, найкраще розглянути способи її експлуатації:

1. Скомпрометовані облікові записи. Поки з ресурсами корпоративної системи працює авторизований користувач, стандартними засобами практично неможливо з'ясувати - чи той це користувач, за якого він себе видає. UBA дозволяє створити профіль для кожного облікового запису, створити базову лінію поведінки і потім виявляти аномалії в діях користувача. Суть полягає в тому, що зловмисник швидше за все не діятиме точно так само як користувач, який втратив даний обліковий запис. Відмінність від звичайної поведінки виступає сигналом для UBA.

2. Зайва допитливість. У будь-якій організації рано чи пізно з'являються інсайдери, що займаються пошуком інформації в корпоративній системі, що представляє собою певну цінність. Це може бути і хакер, який незаконно отримав доступ в корпоративну мережу і займається скануванням ресурсів, щоб виявити інформацію, яку потім буде використовувати для своєї власної вигоди. Якщо співробітник починає занадто активно перебирати вміст мережевих дисків - це як мінімум сигнал для адміністратора безпеки.[3]

3. Виявлення витоків. Одне з можливих завдань UBA – виявлення можливих витоків даних. І знову задається базова типова лінія використання ресурсів та даних, і знову виявляються аномалії в поведінці користувача. Критерієм може бути, наприклад, різке зростання кількості листів з великими вкладеннями, що відправляються на зовнішні поштові адреси.

4. Помилки при налаштуванні доступу. Жодна система повністю не застрахована від впливу людського фактора. Наприклад, під час налаштування правил доступу до ресурсів співробітнику HR-служби помилково надається право на перегляд або навіть редагування конфіденційних початкових кодів програмного коду. UBA при зверненні користувачів до ресурсів дозволяє виявити подібні аномалії.

5. Співробітники, які збираються звільнитися. Для багатьох організацій справжньою проблемою стають співробітники, які мають намір звільнитися. Досить рідко в організації є механізм, що дозволяє поставити співробітника «на контроль» відразу після написання ним заяви про звільнення. UBA має функцію відзначати таких співробітників і потім більш строго відслідковувати використання ними корпоративних ресурсів, виявляти аномалії в поведінці і т.д., що може привести до витоку конфіденційної інформації, розкритті таємниць компанії і т.п.[2]

На основі даних сценаріїв можна визначити загальний алгоритм, за яким працює UBA:

1. Збирає інформацію про типову поведінку користувача, наприклад, виявляє список програм, сайтів, які людина використовує зазвичай на робочому місці.

2. Вибудовує модель типової поведінки.

3. Виявляє аномальну активність і в разі її виникнення моментально реєструє і розцінює як потенційну загрозу для корпоративних ресурсів.

Як джерела даних для UBA/UEBA-систем можуть бути журнали серверних і мережевих компонентів, журнали систем безпеки, журнали з кінцевих вузлів, дані з систем аутентифікації і навіть зміст листування в соціальних мережах, месенджерах і поштових повідомленнях.

Результат роботи UBA/UEBA-систем полягає в тому, що кожен користувач інформаційної системи отримує якийсь так званий «рівень надійності». Адміністратор безпеки, відстежуючи зміну рівнів надійності, може своєчасно реагувати на виявлені за допомогою UBA відхилення від типової поведінки і оперативно вживати заходів для захисту інформаційних ресурсів.

Система аналізу поведінки користувачів і сутностей UEBA (User and Entity Behavior Analytics) - це розширена версія UBA, що дозволяє здійснювати моніторинг не лише окремих осіб, а й пристроїв всередині мережі - всього IT-оточення. За великим рахунком, це нова назва UBA. UEBA-системи збирають дані про хости, мережевий трафік і системи зберігання даних. Це дозволяє проводити аналіз взаємодії операторів і обладнання, забезпечуючи повну видимість робочих процесів, і ідентифікувати більш широкий клас загроз, пов'язаних не тільки з користувачами, але і з об'єктами IT-інфраструктури. Поява нового слова - «Entity» - остаточно закріпила усвідомлення того факту, що для повноцінного аналізу поведінки користувача недостатньо відстежувати тільки його активність. Багато вкрай корисної інформації приносять знання про компанії в цілому, її організаційну структуру, про налаштованих групах доступу і т.д. Крім того, заміна назви класу рішень UBA на UEBA одночасно виключила зі свого складу продукти, призначені для виявлення фінансового шахрайства.

З лідерів світового ринку UBA/UEBA можна виділити таких:

– Exabeam Advanced Analytics (Exabeam) Exabeam.

За заявами самої компанії, Exabeam має найбільшу інсталяційну базу UEBA-систем в світі. На сьогодні компанія позиціонує себе як комплексна платформа для SIEM з розширеною аналітичної функціональністю.

– Forcepoint UEBA.

Рішення Forcepoint User and Entity Behavior Analytics (UEBA) дозволяє командам безпеки проактивно відстежувати всередині організації аномальна поведінка з високим рівнем ризику.

– Splunk User Behaviour Analysis.

Одна з основних переваг Splunk User Behaviour Analysis - виявлення невідомих загроз і аномального поведінки за допомогою машинного навчання.

– Micro Focus Security ArcSight UBA.

Продукт ArcSight User Behavior Analytics надає компаніям детальну інформацію про своїх користувачів, що значно спрощує формування даних про моделі поведінки, що допомагають пом'якшувати загрози. Він допомагає виявляти і розслідувати зловмисне поведінка користувачів, внутрішні загрози та зловживання обліковими записами. [4]

Підсумовуючи, можна стверджувати, що UEBA / UBA-системи - це наступний крок у визначенні невідомих типів загроз, цілеспрямованих атак і внутрішніх порушників. грунтуючись виключно на поведінковому аналізі, ці системи здатні виявляти аномалії і неочевидні взаємодії користувачів з корпоративними системами, що в кінцевому підсумку дозволяє адміністраторам безпеки бачити розширену картину безпеки підприємства та оперативно реагувати на інциденти ІБ.

Список використаних джерел

1.Обзор решений UBA, SIEM, SOAR: в чем различие? /[Електронний ресурс] – Режим доступу: https://www.anti-malware.ru/analytics/Technology_Analysis/UBA-SIEM-SOAR

2. UBA, или щем пользователей с «отклонениями» /[Електронний ресурс] – Режим доступу: https://habr.com/ru/company/inline_tech/blog/303240

Как UEBA помогает повышать уровень кибербезопасности /[Електронний ресурс] – Режим доступу: https://habr.com/ru/company/roi4cio/blog/436082/

3. Обзор рынка систем поведенческого анализа – User and Entity Behavioral Analytics(UBA/UEBA) /[Електронний ресурс] – Режим доступу: https://www.anti-malware.ru/analytics/Market_Analysis/user-and-entity-behavioral-analytics-ubaueba

---

УДК 004.65

СУЧАСНІ ВИМОГИ ДО СИСТЕМ УПРАВЛІННЯ БАЗАМИ ДАНИХ

Бондар В., студ. гр. КБ-171, **Кулініч Р.,** студ. гр. КБ-171
Мехед Д.Б., кандидат педагогічних наук,
доцент кафедри кібербезпеки та математичного моделювання
Чернігівський національний технологічний університет

Актуальність. Кожне сучасне підприємство працює з великою кількістю інформації. В більшості випадків актуальність та доступність цих даних як для працівників, так і для клієнтів відіграють важливу роль в конкурентоспроможності та ефективній діяльності компанії. Зберігання актуальних даних є ключовим завданням для кожної сучасної організації. Зростає потреба в нових, надійніших засобах безпеки БД, здатних задовольнити вимоги до їх продуктивності та масштабованості. На сьогодні існує значна кількість різноманітних СУБД. Відповідно, актуальною постає необхідність комплексного розгляду та систематизації питань вибору оптимальних систем управління базами даних.

Метою дослідження виступає аналіз критеріїв та визначення сучасних вимог до систем управління базами даних.

Питання аналізу особливостей систем управління базами даних висвітлено в багатьох публікаціях закордонних і вітчизняних авторів. Зокрема, основні підходи до оцінки критеріїв та проблем вибору СУБД для побудови інформаційних систем розкриваються в працях: А. А. Аносова [1], М. Т. Фісуна, Є. О. Давиденка [2] та ін.

Завдання аналізу вимог до систем управління базами даних полягає в дослідженні потреб користувачів в зберіганні та оперуванні даними. Важливо враховувати вимоги до функціональності, надійності та доступності, зручність інтерфейсу та усвідомлення очікуваних результатів [3].

Визначення вимог до СУБД, що задовольнятимуть актуальні запити користувачів, ґрунтується на основних критеріях систем управління. При визначенні особливостей СУБД найчастіше використовують наступні групи критеріїв: моделювання даних; особливості архітектури та функціональні можливості; контроль роботи системи; особливості розробки додатків; продуктивність; надійність; вимоги до робочого середовища та змішані критерії.

Щодо *моделювання даних*, серед безлічі моделей найпоширеніші – ієрархічна, мережева, реляційна, об'єктно-реляційна і об'єктна. Вибір моделі залежить від вимог, що визначаються призначенням та галуззю використання баз даних.

Важливою є наявність та властивості тригерів – програм, що викликаються кожного разу при вставці, зміні або видаленні рядка таблиці. Тригери забезпечують перевірку будь-яких змін на коректність, перш ніж ці зміни будуть прийняті.

Деякі сучасні системи мають вбудовані додаткові засоби контекстного пошуку.

Слід також врахувати два фактично незалежних критерії: базові типи даних, закладені в систему, і наявність можливості розширення типів. Якщо відхилення базових наборів типів даних в сучасних