ключ для автентифікації значення хешу при отриманні повідомлення. Ці функції пропонують захист проти атак на прості хешувальні функції [2].

На відміну від симетричних, асиметричні алгоритми шифрування використовують пару споріднених ключів — відкритий та секретний. При цьому, не зважаючи на пов'язаність відкритого та секретного ключа в парі, обчислення секретного ключа на основі відкритого вважається технічно неможливим. В асиметричних криптосистемах, відкритий ключ може вільно розповсюджуватись, в той час як приватний ключ має зберігатись в таємниці. Зазвичай, відкритий ключ використовується для шифрування, в той час як приватний (секретний) ключ використовується для дешифрування. Діффі та Хелман показали, що криптографія з відкритим ключем можлива за умови використання протоколу обміну ключами Діффі-Хелмана [3].

Отже, сучасні дослідження симетричних алгоритмів шифрування зосереджено, в основному, навколо блочних та потокових алгоритмів шифрування та їхнього застосування. Асиметричні алгоритми шифрування використовують пару споріднених ключів — відкритий та секретний.

**Список використаних джерел**

1. https://uk.wikipedia.org/wiki/Криптографія#cite_note-dh2-7
2. https://uk.wikipedia.org/wiki/Шифрування_з_симетричними_ключами
3. https://uk.wikipedia.org/wiki/Асиметричні_алгоритми_шифрування

---

УДК: 004.056.5

## АНАЛІЗ СУЧАСНИХ SIEM ТЕХНОЛОГІЙ

**Соколовська А. А**., здобувачка вищої освіти гр. КБ-171
Науковий керівник: **Мехед Д. Б**., к.п.н., доцент
*Національний університет «Чернігівська політехніка»*

Технологія SIEM (Security information and event management) має на увазі аналіз в реальному часі подій безпеки в мережевих пристроях і додатках. У лінійку рішень SIEM входять різні додатки, прилади та послуги, які застосовуються для збору та аналізу інцидентів інформаційної безпеки.

Число атак за 2020 рік зросло на 59% в порівнянні з аналогічним періодом 2019 року. За моїми спостереженнями, гучні світові події неминуче супроводжуються зростанням числа кібератак, оскільки створюють сприятливий грунт для застосування зловмисниками методів соціальної інженерії. Так, квітень і травень 2020 року стали рекордними за кількістю успішних кібератак. Це можна пов'язати зі складною епідеміологічною та економічною ситуацією в світі, яка припала на ці місяці.

Зловмисники все частіше заражають жертв не одним типом шкідливого ПО, а відразу цілим «букетом» троянів. Так, в ході однієї з масових шкідливих кампаній кіберзлочинці доставляли на скомпрометовані комп'ютери шпигунське програмне забезпечення, ворующее збережені облікові дані з різних додатків.

Проаналізувавши найактуальніші атаки ІБ за 2020 рік можна виділити наступні:

Атаки на 5G. Адже перехід на технології 5G погіршує ситуацію з погрозами для телекомунікаційної галузі, оскільки архітектурні особливості 5G відкривають можливості для нових типів атак на мережі операторів.

Розвиток deep fake. З розвитком технологій штучного інтелекту і нейромереж зловмисники можуть створювати різноманітні інформаційні підробки - deep fake, які можуть використовуватися як для обходу біометричної ідентифікації, так і для обману громадськості та інших цілей.

Зростання атак на хмари. Корпоративні дані, що зберігаються в хмарних сервісах, будуть все частіше бути мішенню атак зловмисників, до яких ті зможуть отримати доступ.

Атаки на RDP. У 2020 році значно збільшилися всі типи атак на RDP (Remote Desktop Protocol). Кіберзлочинці використовують погано налаштовані серверами з RDP або ж експлуатують вразливості протоколу, в залежності від того, що вигідніше для них.

Розвиток кіберуслуг на продаж. Схеми кіберуслуг на продаж розвиваються, набирають обертів і приймають нові форми. Наприклад, набуває більшої популярності схема, коли одні зловмисники зламують інфраструктури компаній і проникають у внутрішню мережу, і далі продають або здають його в оренду іншим учасникам тіньового ринку.

Основним способом захисту є SIEM системи. SIEM-система традиційно застосовується для вирішення проблеми накопичення та оперативної обробки даних про події безпеки, тому першочергові завдання, які вирішуються в рамках кожного пілотного проекту, - це збір, зберігання і обробка подій ІБ. Однак область застосування SIEM-рішення цим не обмежується: за допомогою SIEM-систем вирішуються такі важливі завдання, як виявлення і розслідування інцидентів ІБ, інвентаризація активів, контроль захищеності інформаційних ресурсів. Як правило, список завдань для пілотного проекту визначається на підставі цілей подальшого використання SIEM-системи в компанії.

Протягом останніх років попит на технологію SIEM залишався на високому рівні. Проаналізувавши кілька систем ми можемо виділити наступні найпопулярніші на світовому ринку:

IBM QRadar Security Intelligence Platform включає в себе ряд інтегрованих між собою систем збору подій, моніторингу, аналізу захищеності і розслідування інцидентів.

IBM Security QRadar SIEM має сертифікат ФСТЕК Росії № 3354, який підтверджує виконання функцій моніторингу результатів реєстрації подій безпеки та реагування на них відповідно до вимог Технічних умов.

McAfee Enterprise Security Manager (ESM) поставляється в якості фізичного і віртуального пристроїв і програмного забезпечення. Три основні компоненти, що входять до складу SIEM, - ESM, Event Receiver і Enterprise Log Manager, які можуть бути розгорнуті разом як один екземпляр або окремо для розподілених або великомасштабних середовищ.

Нами було проаналізовано і виявлено такі недоліки:

1) більшість існуючих на даний момент систем не виявляються цілеспрямовані і швидкі масові атаки.

2) не запобігає інціденті, если Виявлено означати Вже відбулося

3) Ще один недолік - високі витрати на вибудовування процесів реагування та експертизу фахівців експлуатації.

Переваги і недоліки - питання стратегії використання. Кожен інструмент призначений для вирішення конкретного завдання і якщо вирішувати з його допомогою іншу задачу, то таке рішення може виявитися неефективним. Є, звичайно, універсальні інструменти, але, якщо ти користуєшся таким інструментом, використовуючи тільки 50% функцій - ви переплачуєте.

На ринку є дуже велика кількість SIEM-рішень, більшість з яких дуже функціональні. Найчастіше їх можливості виходять за межі стандартного визначення SIEM і пропонують клієнтам найрізноманітніші інструменти мережевого менеджменту. Причому багато хто працює прямо «з коробки», вимагаючи мінімального втручання при установці і початковому налаштуванні. Але тут є і заковика: вони можуть відрізнятися за десятками дрібних параметрів, розповісти про які в межах одного огляду не представляється можливим. Тому в кожному конкретному випадку потрібно підбирати рішення не тільки спираючись на головні потреби підприємства, а й враховувати дрібні деталі і майбутнє зростання організації.

**Список використаних джерел**

1. Палівець В. SIEM Analytics [Електронний ресурс] / Валентин Палівець. – 2020. – Режим доступу до ресурсу: http://www.siem.su/review.php

2. Саприкіна А. Огляд світового ринку SIEM систем [Електронний ресурс] / Анастасія Саприкіна. – 2020. – Режим доступу до ресурсу: https://www.anti-malware.ru/analytics/Market_Analysis/overview-global-and-russian-market-siem

3. Порівняння SIEM-систем [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://searchinform.ru/products/siem/sravnenie-siem-sistem/

4. АЛГОРИТМ РОБОТИ SIEM [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://searchinform.ru/products/siem/algoritm-raboty/

---

УДК 004.056.55

## СПОСОБИ ЗАХИСТУ ДАНИХ В CRM СИСТЕМАХ

**Тимошенко Є. М.,** здобувач вищої освіти, гр. МКБ-201
Науковий керівник: **Петренко Т. А.,** к.т.н., доцент
*Національний університет «Чернігівська політехніка»*

CRM система – це поєднання практик, стратегій та технологій, які компанії використовують для управління та аналізу взаємодії із клієнтами та даних протягом життєвого циклу клієнта. Основними завданнями є організація клієнтської бази, автоматизація, управління роботою працівників та управлянні продажами і аналітика. CRM-системи збирають дані про клієнтів за різними каналами або точками контакту між клієнтом та компанією, що може включати веб-сайт компанії, телефон, чат, пряму пошту, маркетингові матеріали та соціальні мережі. Найбільш розповсюдженні сфери, де використовують crm-системи це інтернет-магазини, послуги (від салону краси до клінінг), навчання (курси, мастер-класи, школи), онлайн продажі (одяг, взуття, аксесуари та інше), готелі, ресторани, нерухомість. Проте власники бізнесу в більшості випадках не думають про безпеку даних, які зберігаються в системі. Тому основним завданням є визначити найбільш ефективні способи захисту дані в CRM.

Бекапи - найважливіша річ, про яку нерідко або забувають, або не піклуються. Якщо у вас десктопна система, налаштуйте систему резервного копіювання даних із заданою частотою (наприклад, для RegionSoft CRM це можна реалізувати за допомогою RegionSoft Application Server) і організуйте грамотне зберігання копій. Якщо у вас хмарна CRM, обов'язково до укладення договору дізнайтеся, як організована робота з резервних копій: вам потрібні відомості про глибину і частоті, про місце зберігання, про вартість бекапірованія (нерідко безкоштовні тільки бекапи «останніх даних на період», а повноцінне, секьюрное резервне копіювання здійснюється як платна послуга). Загалом, тут точно не місце для економії або недбалого ставлення. І так, не забувайте перевіряти те, що відновлюється з резервних копій.

Поділ прав доступу на рівні функцій і даних. Безпека на рівні мережі - потрібно дозволити використання CRM тільки всередині офісної підмережі, обмежити доступ для мобільних пристроїв, заборонити роботу з CRM-системою з дому або, що ще гірше, з публічних мереж (коворкінг, кафе, клієнтських офісів та ін.). Особливо будьте обережні з мобільною версією - нехай вона буде лише сильно усіченим варіантом для роботи.

Антивірус зі скануванням в режимі реального часу потрібен в будь-якому випадку, але в разі безпеки корпоративних даних - особливо. Забороніть на рівні політик відключати його самостійно.

Навчання співробітників гігієни кіберпростору - не порожня трата часу, а гостра необхідність. Потрібно донести до всіх колег, що їм важливо не тільки попередити, але і правильно зреагувати на інформацію, що надійшла загрозу. Забороняти користуватися інтернетом або своєю поштою в офісі - це минуле століття і причина гострого негативу, тому доведеться попрацювати саме з профілактикою [1].