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].

Використання коробочної версіїї, замість хмарної. Першим кроком є захист IT-інфраструктури, на якій розміщуються ваші дані CRM. Важливо створити кілька рівнів безпеки, щоб хакерам було все складніше зайти. Ви можете почати з встановлення відомого брандмауера, який дозволить вам контролювати, хто має доступ до ваших даних. Потім встановіть надійну антивірусну програму для захисту даних CRM від вірусів, хробаків та троянських програм. Більшість антивірусних програм забезпечують сканування в режимі реального часу, щоб заблокувати спроби вторгнення, коли вони трапляються, і містять можливості захисту від зловмисного програмного забезпечення та захисту від фішингу, що дозволить вашим співробітникам безпечно переглядати Інтернет.

Вибір надійного постачальника CRM. Мабуть, найважливішим кроком у захисті ваших даних є вибір надійного постачальника CRM. Після того, як ви налаштували свою CRM-систему, пізніше переходити на іншу досить громіздко. Тож ретельно досліджуйте різні CRM-компанії, перш ніж приймати рішення про покупку. Подивіться на надійні IT-сайти новин, такі як Computerworld та CNET, які надають неупереджені огляди та порівняння різних програм CRM. Ваш постачальник CRM повинен надавати необмежений безпечний доступ до ваших даних і мати можливість дотримуватися суворих стандартів даних, викладених у ISO 27001.

Регулярний контроль діяльністі CRM. Вам не потрібно контролювати кожну діяльність ваших співробітників, оскільки вони використовують вашу CRM-систему; однак ви можете встановити попередження про безпеку, які повідомлятимуть вас про несанкціонований доступ або про порушення безпеки. Ви також можете створювати в режимі реального часу інформаційні панелі в режимі реального часу, щоб регулярно контролювати стан безпеки вашої системи CRM та мережі компанії. Багато з цих інструментів інформаційної панелі мають готові можливості для інтеграції з вашою системою безпеки та можуть допомогти вам швидко відстежувати ключові показники безпеки для вашої IT-інфраструктури [2].

Адміністатори CRM мають дотримуватися найкращих практик безпеки. Управління внутрішніми адміністраторами може бути однією з найбільших проблем у впровадженні CRM-безпеки. Співробітники хочуть відчувати, що їм можна довіряти, але ви повинні керувати доступом та рівнями доступу до свого CRM - навіть якщо це означає обмеження доступу адміністратора. Переконатися що працівники використовують власні індивідуальні облікові записи для входу, а не для спільного входу. Крім того, коли працівник залишає компанію, переконайтеся, що термін його входу закінчився або обмежений. Зазвичай ігноруваний ризик безпеки CRM - це можливість завантаження інформації. Хоча багатьом працівникам потрібен доступ до звітування, щоб виконувати свою роботу, **широкий доступ може становити ризик** для цінних даних, що мешкають у вашій CRM. Обмежте кількість осіб, які можуть завантажувати дані, і переконайтеся, що всі знають політику вашої компанії щодо правильного поводження з інформацією [3].

Таким чином, ми проаналізували основні способи захисту даних, які зберігаються в CRM системі, які необхідно вирішити в процесі проектування і побудови інтелектуальних систем розпізнавання кіберзагроз. Без захисту crm системи не можлива повністю безпечна робота підприємства.

Список використаних джерел

1. CRM-системи: захист чи загроза? [Електронний ресурс] / 2 – Режим доступу до ресурсу: https://habr.com/ru/company/regionsoft/blog/445582

2. How to Protect Your Customer Relationship Management (CRM) [Електронний ресурс] – Режим доступу до ресурсу: https://staysafeonline.org/blog/protect-customer-relationship-management-crm-data-hackers.

3. Ways to Secure Your CRM and Avoid Security Risks [Електронний ресурс] – Режим доступу до ресурсу: https://blog.zoominfo.com/crm-privacy-concerns