ЗАХИСТ СЕРВЕРІВ ПРОЦЕСИНГУ КРЕДОБАНКУ

IT.Integrator

Cisco Partner

Замовник: Кредобанк

Галузь: Фінансовий сектор

Рішення: Міжмережеві екрани Cisco Firepower 4110 NGIPS Appliance

БЕЗПЕЧНА РОБОТА ТА ЗАХИСТ ДАНИХ ФІНАНСОВОЇ УСТАНОВИ ЗАЛЕЖАТЬ ВІД РІВНЯ ЗРІЛОСТІ ЇЇ ІНФРАСТРУКТУРИ ТА ВІДМОВОСТІЙКОСТІ КОМПЛЕКСУ КІБЕРБЕЗПЕКИ

Немає жодних сумнівів, що в наших реаліях один зі стратегічних напрямків розвитку банку – це кібербезпека. За неї відповідальна не лише служба IT, але й бізнес загалом, адже захист даних клієнтів, їх надійне зберігання та обробка, конфіденційність проведення банківських операцій залежать від ефективності побудованої системи захисту загалом та цілого комплексу дій і професіоналізму персоналу, зокрема.

Фінансові установи, які дбають про свою репутацію та враховують ризики для бізнесу, старанно слідкують за оновленнями, можливими загрозами та слідують настановам з питань безпеки, які висуває міжнародна спільнота та Національний банк України.

У відповідності до постанови НБУ #95 від 28.09.2017 про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України, зокрема, мова йде про необхідність фільтрації трафіку центрів обробки даних, Кредобанк придбав обладнання та програмне забезпечення для побудови відмовостійкого рішення для захисту серверів процесингу.

Оскільки раніше банк вже відбудував мережеву інфраструктуру дата-центрів на базі архітектури Cisco ACI, оптимально задовольнити його потреби в питаннях якості та відповідності вимогам безпеки трафіку вдалося рішенню Cisco Firepower 4110 NGIPS Appliance.

ЗАХИСТ СЕРВЕРІВ ПРОЦЕСИНГУ КРЕДОБАНКУ

Систему було розгорнуто на двох майданчиках. Обрані міжмережеві екрани слугують сервісними пристроями для фабрики ACI. Основна задача обладнання полягає у інспектуванні трафіку, перенаправлення якого відбувається засобами тієї ж таки фабрики ACI. Самі міжмережеві екрани реалізовані, як окремі логічні пристрої у режимі multi-instance на гіпервізорах Firepower 4110.

Технологія «failover» дозволила об'єднати усі міжмережеві екрани в одну логічну систему. Інтерфейси керування платформами, самими міжмережевими екранами та інтерфейси для failover – усі підключені до класичної мережі, а керування цими пристроями здійснюється з існуючої системи FMC.

Інформаційна взаємодія між компонентами системи на мережевому рівні відбувається за допомогою використання протоколів на базі відкритих стандартів, що входять до протоколу IP. А інформаційний обмін між системами відбувається через єдине інформаційне середовище, використовуючи стандартні протоколи обміну даних із забезпеченням необхідної кількості оптичних каналів зв'язку між пристроями.

В результаті розроблені технічні рішення забезпечують функціонування системи безперервно, в цілодобовому режимі, 365 днів на рік. Система забезпечує високу ступінь готовності, спроєктована з відсутністю єдиних точок відмови для критичних, з точки зору функціонування, елементів.

Відмовостійкість забезпечується наступними засобами:

- Використання високонадійного обладнання
- Дублювання і резервування ліній зв'язку
- Дублювання і резервування критичних для роботи системи в цілому програмних, програмно-апаратних та апаратних засобів.

Для забезпечення інформаційної безпеки на міжмережевих екранах були налаштовані наступні політики безпеки:

- Політика фільтрації трафіку від / до мережі процесингу на рівні L4-L7. Ця політика була перенесена із існуючого контексту міжмережевого екрану ASA для мережі процесингу.
- IPS політика для мережі процесингу.
- Політика фільтрації на базі переліків потенційно-небезпечних FQDN/адрес, що динамічно завантажуються.

Як результат, Кредобанк отримав комплексну систему для захисту серверів процесингу на платформі Cisco Firepower 4110 NGIPS Appliance, до складу якої було включено якісне відмовостійке обладнання, програмне забезпечення, яке відповідає IT та бізнес-вимогам установи.

Артур Цесляр (Artur Cieslar), заступник голови правління Кредобанку:

«Кредобанк завжди працює відповідно до європейських стандартів та згідно з ними підтримує на безпечному рівні свої системи та інфраструктуру. Банк приділяє максимальну увагу захисту фінансової інформації та веде активну роботу як всередині установи, розвиваючи власну інфраструктуру, так і зовнішню. Тож, ми плануємо і надалі постійно працювати над впровадженням сучасних технологій, щоб наш банк відповідав найвищим стандартам безпеки та якості фінансових послуг».

Дмитро Жуковський, директор департаменту інформаційних технологій «IT-Інтегратор»:

«Наша команда має поважний досвід проєктів в напрямку впровадження архітектури Cisco ACI, в тому числі, у банківському секторі, а також інтеграції продуктів Cisco Security, що дозволяє нам демонструвати високу продуктивність та оперувати реальними кейсами з практики. Маємо відзначити, що такі проєкти - завжди новий виклик та поштовх до вдосконалення. Кредобанк вже багато років демонструє високопрофесійний підхід до організації IT-інфраструктури та комплексу безпеки. Пандемія лише трохи пришвидшила цифровізацію сервісів та розробку віддалених послуг, і наразі вже 98% бізнес-процесів банку працюють онлайн».