Система відеоменеджменту SecurOS™/ Аналітична платформа

Керівництво з кібербезпеки

v. 1.3

4січня 2021 року

1. Вступ

ISS взяла на себе зобов'язання впровадити необхідні функції захисту даних для забезпечення найвищого рівня безпеки будь-якої системи ISS. Системи сьогодні, як правило, мають доступ до певного типу мережі, що підвищує важливість кібербезпеки. ISS впровадила ряд функцій кібербезпеки для зниження зростаючого ризику кіберзагроз. Нижче наведено більш докладні відомості про деякі функції кібербезпеки платформи SecurOS ™.

2. Захист паролів

Захист паролів, що зберігаються в SecurOS і використовуються в мережі для обміну між серверами, клієнтами та IP-камерами SecurOS, є дуже важливою частиною кібербезпеки.

1. Всі паролі, що зберігаються в SecurOS для цілей аутентифікації на IP-камерах, зберігаються у вигляді зашифрованих даних (через AES-256) на сервері ISS.
    a. SecurOS підтримує авторизацію дайджесту для більшості постачальників камер, що підтримують таку функцію.
2. Паролі, що передаються по мережі, шифруються з використанням хешу на основі сеансу (SHA-2).
3. Паролі, що використовуються для вбудованого управління правами користувачів SecurOS, також зберігаються в зашифрованому вигляді (через AES-256) в базі даних SQL SecurOS.
4. Для забезпечення іншого рівня безпеки SecurOS може підключатися до сервера Active Directory або LDAP для аутентифікації своїх користувачів. У цьому випадку всі дані пароля будуть збережені і захищені AD сервером.
5. Для паролів, що використовуються користувачами Windows на серверах/робочих станціях ISS, рекомендується дотримуватися суворої політики паролів Windows.

3. Аутентифікація

SecurOS гарантує, що всі процедури аутентифікації в системі захищені.

3.1. Вбудоване управління правами користувачів

Використовуючи управління правами користувачів SecurOS, створіть власних користувачів SecurOS з різними дозволами. Обмежте кількість користувачів-адміністраторів. Для користувачів оператора обмежте те, що оператор може бачити в інтерфейсі, тільки тими компонентами, які необхідні оператору для виконання своєї роботи.

3.2. Інтеграція LDAP/LDAPS/Active Directory

SecurOS підтримує інтеграцію з Active Directory і LDAP. В якості альтернативи використанню власних користувачів SecurOS, користувачі AD або LDAP можуть підключатися до системи SecurOS, використовуючи дозволи, налаштовані в управлінні правами користувачів SecurOS.

Для додаткової безпеки, SecurOS також підтримує LDAP через TLS, також відомий як LDAPS. LDAPS дозволяє шифрувати дані LDAP (включаючи облікові дані користувача) при передачі, коли встановлюється прив'язка до каталогу, тим самим захищаючи від

крадіжки облікових даних.

3.3. Безпека авторизації

SecurOS підтримує обмежену кількість і затримку між спробами аутентифікації користувача. Після 3 невдалих спроб входу в систему користувач блокується від повторної спроби входу в систему протягом 30 секунд.

3.4. Авторизація на основі пароля для підключення MCC

SecurOS вимагає, щоб користувачі-адміністратори вводили пароль на віддаленому сайті і на сервері MCC для завершення процесу авторизації.

4. Безпека PostgreSQL

PostgreSQL, яка є базою даних SQL SecurOS для зберігання даних, поставляється з вбудованою авторизацією. PG Admin, який є інструментом для доступу до даних і виконання функцій адміністратора БД, захищений паролем, і будь-які встановлені рядки підключення від SecurOS до PostgreSQL вимагають дійсного імені користувача і пароля.

ISS рекомендує змінити пароль користувача PostgreSQL за замовчуванням.

5. Захищена ідентифікація сервера/робочої станції SecurOS

Всі сервери відео/управління SecurOS перевіряють свою особистість в системі 2 способами:

- У системному ліцензійному ключі за допомогою коду USB Guardant або хешу серверного обладнання.
- По їх імені NetBIOS в конфігурації системи.

Всі клієнти робочої станції оператора SecurOS можуть ідентифікувати себе в конфігурації 2 способами:

- По їх імені NetBIOS.
- За їх IP-адресою (клієнтські підключення можуть бути обмежені зумовленими IP-адресами).

6. Шифрування для даних в місцях зберігання

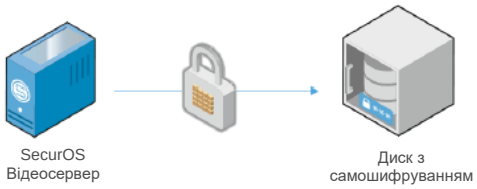
Для забезпечення захисту даних в місцях зберігання використовується шифрування.

SecurOS підтримує 2 типи методів шифрування даних:

- Шифрування жорсткого диска з використанням дисків SED.
- Шифрування бази даних.

Шифрування диска SED:

ISS підтримує використання сертифікованої технології апаратного прискорення шифрування за допомогою дисків з самошифруванням. Записи відео і метаданих можуть бути зашифровані за допомогою дисків і контролерів, сумісних з SED. Технологія диска з самошифруванням заснована на виділеному чіпі для шифрування всіх даних за допомогою AES-128 або AES-256 і не займає ресурсів процесора. Технологія SED відповідає федеральним стандартам обробки інформації (FIPS) 140-2/140-3.



Шифрування бази даних:

ISS підтримує шифрування бази даних для певних даних SecurOS. Всі персональні дані, що зберігаються в модулі SecurOS FaceX, шифруються в стані спокою за допомогою шифрування PostgeSQL.

7. Цифровий підпис і шифрування експортованого відео

Якщо відеодані експортуються з SecurOS, необхідно забезпечити справжність експортованого відео.

1. SecurOS підтримує цифрові сертифікати для експортованого відео. Сертифікати використовуються для перевірки автентичності джерела експортованого відео, наданого правоохоронним органам як доказ для використання в суді. Можна використовувати або довірений сертифікат, виданий центром сертифікації, або сертифікати, видані самостійно.
2. Експортовані файли підписуються цифровим підписом з використанням сертифіката, встановленого на сервері/робочої станції експортера, а також з додаванням спеціальних метаданих SecurOS, таких як обліковий запис користувача, ідентифікатор камери і т. д... Це дозволяє довести джерело доказів і гарантувати цілісність даних (що відео жодним чином не було підроблено і змінено). Цифрові підписи можна перевірити за допомогою диспетчера доказів SecurOS або утиліти перевірки цифрового підпису SecurOS.
    a. Сертифікат, який використовується для підпису, присвоюється певному профілю конвертера архівів (модуль SecurOS для експорту відео).
    b. Існує додатковий рівень захисту, коли сертифікат вимагає пароля для підпису чого-небудь (може бути налаштований адміністратором або введений оператором вручну).
3. Існує опція, що дозволяє шифрувати експортовані файли за допомогою будь-якого постачальника шифрування, встановленого в Windows (наприклад, AES-256), таким чином захищаючи файли від несанкціонованого доступу.

8. Захищений Зв'язок SecurOS

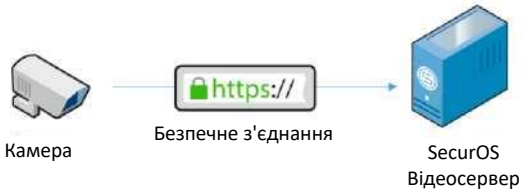
8.1. Безпечне з'єднання між камерами і серверами запису

Захист відеоданих, переданих з IP-камер на сервери відеозапису/клієнтські робочі станції, є найважливішим завданням безпеки в більшості сучасних установок. Це завдання стає ще більш важливим у великих системах, які можуть включати велику кількість камер, серверів, локальних/віддалених клієнтів та декілька мережевих інфраструктур.

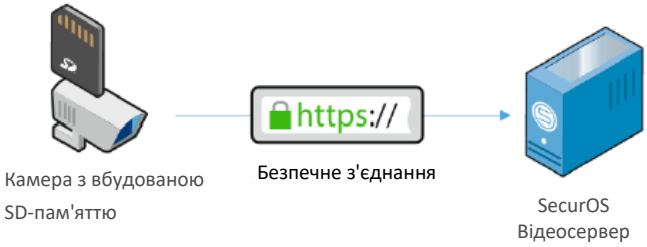
1. SecurOS підтримує цифрові сертифікати камери для більшості основних постачальників камер, що підтримують цю функцію. Сертифікати, встановленим в камерах, повинні бути довіреними для відеосерверів SecurOS.
    a. Тільки пристроям з довіреними сертифікатами дозволено підключатися до SecurOS.
    b. Відносини довіри управляються системним адміністратором за допомогою сховища сертифікатів Windows.

2. SecurOS підтримує дайджест-аутентифікацію (фактичний пароль ніколи не передається по мережі).

3. SecurOS забезпечує безпечне з'єднання (зашифроване і перевірене джерелом) між камерою і відеосервером з використанням тунелювання HTTPS.
    a. Більш конкретно, дані RTSP і RTP тунелюються через HTTPS.
    b. HTTP-транспорт побудований з двох окремих HTTP-запитів GET І POST, ініційованих клієнтом. Між сервером і камерою будуть встановлені два окремих з'єднання. Потім сервер зв'яже з'єднання, щоб сформувати віртуальне повнодуплексне з'єднання.
    c. Аудіо також зашифровано.
    d. Встановіть сеанс по протоколу HTTPS (захищена авторизація (по протоколу TLS) з встановленим в камері довіреним сертифікатом). Це захищає дані користувача.



    e. Спочатку на стороні камери повинен бути включений протокол HTTPS. Потім на стороні системи відеоменеджменту SecurOS необхідно включити настройку для використання шифрування камери.
    f. Тунелювання HTTPS також підтримується для синхронізації Securos



EdgeStorage (модуль ISS для вилучення відео з SD-карти камери).

8.2. Безпечне з'єднання між усіма серверами SecurOS

SecurOS підтримує безпечне з'єднання з використанням протоколу TLS 1.2 між усіма серверами SecurOS в системі.

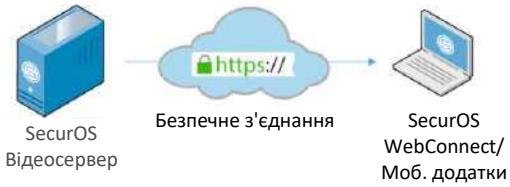
8.3. Безпечне з'єднання між серверами SecurOS і "товстими клієнтами"

SecurOS підтримує безпечне з'єднання з використанням протоколу TLS 1.2 між усіма серверами SecurOS і "товстими клієнтами" в системі.

8.4. Безпечне з'єднання між серверами SecurOS і "тонкими клієнтами"

SecurOS підтримує безпечне HTTPS-з'єднання між серверами SecurOS і "тонкими клієнтами" SecurOS (SecurOS WebConnect або SecurOS Mobile). Слід враховувати наступні додаткові вимоги до безпеки:

1. Використовуйте HTTPS-з'єднання з довіреним сертифікатом. Для підключення сервера по протоколу HTTPS потрібен сертифікат TLS. Для установки сертифіката необхідно виконати наступне:
   a. Довірений сертифікат TLS встановлюється у ваше особисте сховище сертифікатів за допомогою оснащення MMC.
   b. Якщо у вас вже є сертифікат для веб -/мобільного сервера SecurOS, рекомендується використовувати його.
   c. Якщо ні, довірений сертифікат можна отримати у будь-якого довіреного центру.
2. Рекомендується використовувати виділений веб-/мобільний сервер SecurOS для забезпечення доступу операторів, що підключаються по глобальній мережі.
3. Всі мережеві порти, за винятком тих, які необхідні для роботи веб-/мобільних модулів, повинні бути заблоковані в глобальній мережі.
4. Права *користувача* SecurOS повинні бути налаштовані для запобігання несанкціонованого доступу до *камер* SecurOS при вході в систему з веб-клієнта або мобільного додатку.
5. Незахищені (паролі повинні відповідати стандартним вимогам складності і бути унікальними) або скомпрометовані облікові дані ніколи не повинні використовуватися користувачами SecurOS для запобігання несанкціонованому доступу.



8.5. Відмовостійкий кластер SecurOS – безпечне з'єднання

З'єднання між диспетчером сервера і вузлом кластера зашифровано і вимагає авторизації під управлінням адміністратора Windows.