Кіберзахист для систем безпеки та центрів керування

Комплексне рішення для критичної інфраструктури

Згідно з Постановою Кабінету Міністрів України від 19.06.2019р. №518 заходи з кіберзахисту на об'єктах критичної інформаційної інфраструктури (ОКІІ) об'єкта критичної інфраструктури, повинні забезпечувати:

- формування на об'єкті критичної інфраструктури загальної політики інформаційної безпеки;
- управління доступом користувачів та адміністраторів до об'єктів захисту ОКІІ;
- ідентифікацію та автентифікацію користувачів та адміністраторів ОКІІ;
- реєстрацію подій компонентами ОКІІ та їх періодичний аудит;
- мережевий захист компонентів та інформаційних ресурсів ОКІІ;
- доступність та відмовостійкість компонентів та інформаційних ресурсів ОКІІ;
- визначення умов використання змінних (зовнішніх) пристроїв та носіїв інформації на ОКІІ;
- визначення умов використання програмного та апаратного забезпечення ОКІІ;
- визначення умов розміщення компонентів ОКІІ.

Захисту потребують не тільки інформаційні системи:

- **Системи безпеки** (моніторингові центри, АРМ операторів, сервери, мережева інфраструктура, мережеве обладнання систем безпеки).
- **Центри керування критичними процесами** (центральні пульти керування, диспетчерські вузли, АРМ операторів, сервери, SCADA тощо).

AM Integrator Group | www.amintegrator.com | mail@amintegrator.com
Київ, вул. Іллінська, буд. 14/6 | +38 (044) 394-86-07, 394-86-09

Оцініть, наскільки захищені ваші критичні системи з погляду інформаційної безпеки

Загрози	Вимоги	Еталон	У Вас?
Автентифікація за чужим логіном/паролем	• ідентифікація та автентифікація користувачів та адміністраторів; • використання багатофакторних систем ідентифікації (в т.ч. біометричних).	✓	○
Відсутність резервних копій баз даних	• налаштування автоматичного створення бекапів критичних сервісів та БД.	✓	○
Підключення зовнішнього каналу зв'язку, злом, атака внутрішньої мережі з будь-якого IP пристрою (ПК, контролер, відеокамера тощо) через відкриті фізичні порти або через доступ до центрального сервера	• відключення можливості роботи з зовнішніми пристроями; • налаштування списків дозволеного ПЗ; • мережевий захист компонентів та інформаційних ресурсів; • визначення умов використання змінних (зовнішніх) пристроїв та носіїв інформації.	✓	○
Неконтрольований доступ до серверних та операторських приміщень, компонентів системи	• забезпечення контролю доступу до приміщень та компонентів системи засобами СКУД та СУІБ.	✓	○
Виведення системи з ладу внаслідок ненавмисних, помилкових дій персоналу	• розробка комплексних організаційних та технічних заходів.	✓	○
Загроза втрати управління, контролю, прав адміністрування, відсутність дублювання та заміщення ролей.	• контроль, моніторинг, протоколювання привілейованого доступу користувачів; • наявність власного сховища паролів доступу; • використання системи резервного копіювання даних.	✓	○
Відсутність живлення	• використання джерел безперебійного та резервного живлення для критичних компонентів системи;	✓	○
Наявність нелегітимної активності усередині мережі.	• моніторинг та аналіз аномального трафіку та подій; • виконання заходів з сповіщення та протидії загрозі.	✓	○
Несанкціоноване копіювання відео та мета-даних системи з локального АРМ	• запобігання загрозі неконтрольованої передачі або втрати інформації; • використання засобів шифрування носіїв.	✓	○
Використання вразливостей системи (в т.ч. відомих)	• контроль вразливості операційних систем, сервісів що виконуються та апаратних засобів.	✓	○
Відмовостійкість системи	• дублювання серверів, критичного обладнання, сервісів та баз даних; • використання системи резервного копіювання даних, операційних систем.	✓	○
Відсутність актуальних прошивок / оновлень ОС та додатків підвищує ризик злому системи	• визначення умов використання ПЗ; • розгортання локального центру оновлення ПЗ; • односторонній доступ до зовнішніх центрів оновлень.	✓	○

Ми розробили РІШЕННЯ з комплексного захисту від кібератак для інженерних систем і систем фізичної безпеки та готові надати послуги з їх впровадження.

Чому AM Інтегратор Груп?

Компанія AM Інтегратор Груп працює на ринку системної інтеграції України більше 30 років. Одне з напрямків діяльності компанії – успішне проєктування і впровадження систем IT-інфраструктури та безпеки провідних світових вендорів, забезпечення комплексного захисту інформаційних ресурсів. Компанія має штат сертифікованих співробітників, відповідні статуси і досвід.

AM Integrator Group | www.amintegrator.com | mail@amintegrator.com
Київ, вул. Іллінська, буд. 14/6 | +38 (044) 394-86-07, 394-86-09