Рекомендації
щодо підвищення безпеки інформаційно-телекомунікаційних систем із використанням IP-відеокамер

1) Зміна та підвищення стійкості до зламу паролів доменних та локальних користувачів "Парольна політика", які мають доступ до камер-відеоспостереження

1.1 впровадження нових вимог до довжини, складності та терміну дії паролю в налаштуваннях корпоративних сервісів - зменшення ризику підбору паролів користувачів;

1.2 зміна паролів всім обліковим записам користувачів особливо з адміністративними повноваженнями;

1.3 внесення змін в парольну політику Active Directory щодо нових вимог до паролів (використанням щонайменше 14 символів, використання спецсимволів, зміна паролів усім користувачам на періодичній основі(1-2 рази на місяць) т.п.)

2) Оновлення старих версій та переустановлення не підтримуваних версій ОС програмного забезпечення, яке використовується для функціонування камер-відеоспостереження

2.1 постійний контроль за процесом оновлення старих версій програмних продуктів які використовуються в інфраструктурі;

2.2 у разі припинення випуску оновлень виробником ОС/ПЗ, яке використовується в інфраструктурі, розглянути можливість його заміни альтернативним ОС/ПЗ;

2.3 провести інвентаризацію використовуваних програмних продуктів в середині мережі, з метою недопущення використання та впровадження програмних продуктів сумнівного походження, які можуть становити ризики несанкціонованого проникнення чи отримання контролю третіми особами.

3) Оновлення старих версій та переустановлення не підтримуваних ОС для систем зберігання та накопичення відеоматеріалів, здійснення постійного контролю систем на яких не можливо змінити ОС "Старі версії ОС Windows"

3.1 постійний контроль за процесом оновлення старих версій ОС та програмних продуктів які використовуються в інфраструктурі;

3.2 у разі припинення випуску оновлень виробником ОС/ПЗ, яке використовується в інфраструктурі, розглянути можливість його заміни альтернативним ОС/ПЗ, у разі не можливості замінити, з використанням мережевого обладнання та продукту ERD організувати контроль за такими ОС;

3.3 провести інвентаризацію використовуваних програмних продуктів в середині мережі, з метою недопущення використання та впровадження програмних продуктів сумнівного походження, які можуть становити ризики несанкціонованого проникнення чи отримання контролю третіми особами.

4) постійний контроль та розмежування привілейованих облікових записів, сервісних та звичайних з правами користувача

4.1 контроль за допомогою систем безпеки, функціональних можливостей AD, питань надання окремим користувачам додаткових привілеїв (системи контролю/фіксації із зазначенням періоду);

4.2 Контроль за створенням нових облікових записів, у т.ч. локальних, та блокування/видалення облікових записів, які не використовуються;

4.3 Розмежування порядку доступу з використанням функціональних можливостей AD та мережевого обладнання (політики щодо доступу окремих робочих станцій/серверів).

5) обов'язкова потреба до "Впровадження корпоративного VPN"

5.1 впровадження корпоративного VPN

5.2 впровадження механізму двофакторної автентифікації при підключенні до корпоративного VPN, або інші тимчасові варіанти реалізації (сертифікати, сервіси CISCO, сервіси Microsoft) до того часу як буде реалізовано 2FA;

6) контроль облікових записів, стосовно яких здійснюються постійні спроби підбору паролів, у т.ч. на різних публічних сервісах компанії (підприємства/установи)

6.1 враховуючи різні можливі методи, що можуть бути використані зловмисниками, як і постійного потокового підбору так і з використанням інтервальної активності (свідчить про можливе використання автоматизації - скриптів);

6.2 унеможливити використання звичайними користувачами облікових записів з адміністративними привілеями, у т.ч. локального адміністратора.

7) обмежити доступ до пристроїв тільки з конкретних IP-адрес, сформувати білий список таких адрес

8) виконати рекомендацій виробника пристрою з посилення рівня захищеності веб-камер та обладнання, що працює з відеосигналом