## Сесія запитань та відповідей №5

1. **Який інструмент (програмний продукт) ви використовуєте в Roosh для інвентаризації, зберігання та актуалізації інформації про Активи?**

У випадку із роботою з CISO as a Service підійде продукт для колаборації, планування, зберігання табличних та текстових даних і документів. Це питання зручності, або питання до сервіс провайдера, який має досвід використання певного набору інструментів із опрацьованим контентом та робочим процесом.

Ми в Roosh використовуємо для цих цілей Notion. Цей інструмент зручний тим, що в ньому можливо побудувати достатньо складну систему пов'язаних між собою баз даних і потім фільтрувати, сортувати та групувати ці дані за різними критеріями.

2. **З вашого досвіду за рік розбудови кібербезпеки який відсоток виконання плану був на рік переосмислення?**

За рік розбудови системи кібербезпеки ми виконали поставлений план приблизно на 90%. Після повторної оцінки ризиків зрозуміли, що по деякім опрацьованим загрозам не велося достатньої кількості підтримуючих робіт і їх потрібно заново пропрацювати, тому чесною цифрою буде десь 80-85%.

3. **Як можна забезпечити захист конфіденційних даних, до яких має доступ велика кількість користувачів просто за робочими обов'язками?**

    1. Потрібно сегментувати дані, побудувати матрицю активів даних.
    2. Сегментувати користувачів, побудувати матрицю ролей, в матриці ролей визначити доступ певної ролі до певного типу даних.
    3. Обмежити доступ всіх інших користувачів до певного типу даних поза роллю.
    4. Визначити та контролювати тип доступу (читання, редагування, створення та видалення) ролі до даних в рамках штатних повноважень.
    5. Як це буде завершено - становити цикли перегляду доступів і ролей.

Для цього можна використовувати стандартні технології з комплекту business collaboration Google чи Microsoft. Є додаткові технології інвентаризацією та управління доступом, які автоматизують та полегшують цей процес.

4. **Враховуєте ви, що хтось із вашої компанії може бути куплений з метою злити дані**

Ці типи ризиків з категорії злонамірена інсайдерська активність. Із цими ризиками можна боротись шляхами сегрегації повноважень і доступів, моніторингу активності, шифрування даних, перехоплення інформаційних витоків і так далі.

5. **А чи не є порушенням принципів безпеки коли деякі рішення чи способи реалізації цих рішень делеговані системному адміністратору? Наскільки я знаю об'єднання людини, що адмініструє, та тієї, що забезпечує безпеку, неприпустимо.**

Так, це порушення базових принципів. Має бути сегрегація повноважень.

Що стосується операційного процесу - існує принцип “чотирьох рук”, коли адміністратор вносить зміни, а офіцер безпеки ці зміни затверджує. Або коли адміністратор запитує доступ, а офіцер безпеки схвалює доступ на сервісну сесію.

6. **Чи є якась методологія впровадження тих, чи інших продуктів на різних етапах створення кібербезпеки для підприємства? Які інструменти краще впроваджувати?**

Правильна методологія - це ризикоорієнтований підхід та принцип раціональності.

Перше - це визначення ризиків, їх пріоритизація та потім - впровадження технологій та підходів для зменшення спочатку пріоритетних ризиків.

Принцип раціональності - вартість засобів та заходів для нейтралізації ризиків не має перевищувати вартості наслідків від настання ризиків.

7. **Використовували MDM для чого конкретніше?**

Перш за все ми використовуємо MDM для того, щоб мати можливість централізовано встановлювати користувачам необхідні програми, важливі оновлення і тд. Наприклад, корпоративний антивірус ми розгортали саме за допомогою MDM. Оскільки наші спеціалісти працюють з різних локацій, MDM також надає можливість віддалено діагностувати та усувати проблеми, які виникають в користувачів.

Тут окремо зазначу, що хоча MDM інструменти зазвичай надають можливість непомітно щось встановлювати чи вмикати певні специфічні налаштування на пристроях користувачів, ми цього не робимо. Для нас важлива чесність і прозорість в комунікаціях, тому про кожне оновлення чи встановлення нової програми через MDM ми попереджаємо користувачів в загальних чатах.

8. **Антивірус ESET NOD коштує 1000 гривень на рік на одну робочу станцію. На сервер приблизно 3000 гривень. Сто робочих станцій + 10 серверів = 130 тисяч на рік. Так, це дуже дешево.**

Антивірусний захист - це базовий інструмент, наразі він вбудований в сучасні операційні системи, але не гарантує захисту від шкідливого програмного забезпечення та компрометації облікового запису користувача.

9. **Добрий вечір. Нещодавній злом роботів пилососів з доступом до його камери, динаміків і мікрофона довів, що тут гостьова мережа WiFi не врятує від витоку даних. У зловмисників вдалося зробити шпигуна на колесах всередині компанії.**

Так, зловмисник може отримати відеоканал та звуковий канал від робота пилососа.

Це ризик, але для компанії це НЕ критичний ризик, за виключенням:

- Цінна документація НЕ розкидана по підлозі, де пилосос може її прочитати
- Важливі переговори НЕ ведуться в коморі де знаходиться пилосос

Цей ризик більш критичний до приватності, але НЕ для конфіденційності.