Сесія запитань та відповідей. Тренінг №1

1. Чи використовуєте ви віртуальні машини? На скільки вони дієві для захисту?

Віртуальні машини були створені для оптимізації ресурсів апаратного забезпечення, але будучи ефективним інструментом для ізоляції систем мають суттєві переваги для кібербезпеки. Вони створюють окремі середовища, що дозволяє мінімізувати ризик поширення загроз на фізичний сервер або інші віртуальні машини у випадку кібератаки. Особливо корисні для тестування потенційно небезпечних програм або оновлень без ризику для основних систем. Однак варто зазначити, що без належного налаштування та захисту гіпервізора вони можуть бути вразливими до атак. Іншими словами, віртуальна машина є такою ж операційною системою, що й фізична, тому всі загрози також актуальні й для VM. Будучи віртуальною, вона не гарантує захист від компрометації, але все ж є ефективним способом ізоляції для захисту фізичних ресурсів ПК чи сервера. Тому інтеграція VM повинна супроводжуватися використанням засобів захисту та моніторингу.

2. Питання для малого бізнесу, яким чином себе захистити, якщо малий бізнес тільки розвивається і на сьогодні не має достатньо коштів та можливостей на захист?

Кожна компанія, включно з великими, стикається з нестачею ресурсів для забезпечення якісної кібербезпеки. Для малого бізнесу це ще складніше, оскільки операційні процеси часто не мають чіткої структури, що ускладнює впровадження контролів кібер- та інформаційної безпеки.

Очевидно, що видатки, які може дозволити МСБ, є меншими від можливостей великого бізнесу. Однак, будь-яка кібербезпека починається з інвентаризації активів, оцінки ризиків, розробки заходів кіберзахисту та перетворення цих заходів на зрозумілі завдання для впровадження. Ці активності не завжди вимагають прямих інвестицій, а базовий набір інструментів з кібербезпеки можна зібрати за доступні кошти.

Метою цього курсу є надання методологій, які дозволять значно покращити кібербезпеку та оптимізувати витрати на цей процес. Рекомендуємо прослухати курс до кінця, щоб зрозуміти, як ефективно використовувати доступні ресурси.

3. Приклад корпоративного антивірусу, який ви можете порекомендувати?

На цьому курсі ми не радимо конкретні технології, радше надаємо методології, як обрати саме ті, які вам найбільше підходять. Ми рекомендуємо звернутись до визнаних рейтингів, наприклад, від аналітичної компанії Gartner: https://www.gartner.com/reviews/market/endpoint-protection-platforms.

Ми зосереджуємося на наданні знань, які допоможуть вам вибрати оптимальні рішення для вашої конкретної ситуації. Важливо розуміти, що всі рішення по безпеці комп'ютерів дуже схожі і водночас відрізняються.

Необхідно враховувати особливості вашої інфраструктури (наприклад, під які ОС має бути агент), а також побудову процесу моніторингу. Сучасний антивірус може лише підсвітити проблему, але саме аналітик повинен виконати incident response, який може бути реалізований багатьма способами. В тому числі зовнішньою командою SOC.

Загальна рекомендація - обрати виробника, який підходить під вашу інфраструктуру і має багатий вибір додаткових функцій, а також різноманіття рівнів підписок - чим дорожче підписка, тим більше функцій ви матимете. Почніть з базової підписки, розбудуйте процес виявлення і реагування на загрози, а коли поточної функціональності буде недостатньо - розгляньте більш функціональну підписку.

4. Для українського ринку будуть ефективніші стандарти ДСТУ, КСЗІ чи NIST? Наскільки наші та американські стандарти схожі?

Українські законодавці завжди засновувалися на західних практиках і методологіях, зокрема, КСЗІ також засновується на фреймворку Common Criteria, який було розроблено в Канаді. Тому можна сказати що основні принципи і засади схожі.

Водночас, КСЗІ є достатньо глибоким та якісним фреймворком, але складним для впровадження і підтримки, і не завжди відповідає сучасним вимогам гнучкості та високої динаміки змін в інфраструктурі.

Українські регулятори вже допускають використання ISO 27001 або NIST для деяких компаній критичної інфраструктури замість КСЗІ. Якщо від вас, як невеликої компанії, явно не вимагають відповідність КСЗІ, краще взяти за основу ISO 27001 або NIST.

5. Чому кіберполіція і інші подібні організації відправляють смс повідомлення, з якою метою саме через смс? через простоту? Якщо так, то наскільки це безпечно?

Використання SMS для сповіщень пояснюється простотою та доступністю цього каналу. Усі телефони підтримують SMS, що робить цей спосіб доступним навіть без інтернету. Однак, цей канал має свої вразливості, оскільки SMS можуть бути перехоплені через атаки на мобільні мережі. Тому держані органи використовують SMS виключно в якості каналу оповіщення, а не інтерактивної взаємодії з громадянами.

6. Чи простіше використати антивірус Cisco Umbrella, який по вартості дешевше чим Eset Enterprise для захисту? І 2 питання КСЗІ скоро будуть всі установи проходити, але чи їхній висновок дасть впевненість, що твоя компанія дійсно захищена?

Cisco Umbrella є чудовим варіантом для захисту мережі через DNS-фільтрацію та хмарні технології, що робить його доступнішим і зручнішим для малого та середнього бізнесу. ESET Enterprise, в свою чергу, пропонує більш глибокий захист кінцевих точок завдяки широким можливостям керування ними та різноманітним методам виявлення загроз. Вибір між цими рішеннями залежить від конкретних потреб і особливостей вашої інфраструктури.

Висновок КСЗІ підтверджує відповідність вашої організації певним стандартам безпеки, проте це не гарантує повний захист від усіх можливих загроз. У світі інформаційної та кібербезпеки поняття "повний захист" не використовується, оскільки 100% безпеки можливе лише у вимкненого комп'ютера. В інших випадках ми говоримо про зниження ризиків і управління ймовірностями реалізації загроз.

7. Питання по ресурсу Cisco Umbrella, на скільки надійно можна захиститися використовувати даний сервіс?

Cisco Umbrella забезпечує високий рівень захисту, особливо на початкових етапах — блокування шкідливих сайтів та DNS-запитів ще до того, як загроза проникне в мережу. Це ефективне рішення для захисту від фішингових атак і запобігання шкідливому програмному забезпеченню. Однак, для повної безпеки рекомендується комбінувати його з іншими засобами, такими як антивіруси та засоби моніторингу мережі.

8. Яка орієнтовно частка компаній малого та середнього бізнесу, які потрапили "під роздачу" в цьому році? Чи зменшується вона з кожним роком саме в Україні чи навпаки зростає?

Згідно з останніми даними, приблизно 46% усіх кібератак спрямовані на компанії малого та середнього бізнесу. Тенденція до зростання таких атак залишається стабільною, з кожним роком кількість інцидентів збільшується, особливо в умовах гібридної війни, де атаки на критичну інфраструктуру є частими.

9. Як централізовано дізнатись всі поштові скриньки, якими люди користуються? Особливо коли користувачів інтернет більше ніж 100 ?

Для корпоративних скриньок завдання можна вирішити через централізовані інструменти управління електронною поштою, наприклад, Office 365 або Google Workspace, де адміністратор може отримати повний доступ до всіх поштових скриньок і користувачів.

Якщо йдеться про персональні скриньки, які співробітники використовують для роботи, це питання краще вирішити на рівні політик компанії, пояснюючи, що для робочої діяльності слід використовувати корпоративні скриньки. За наявності централізованого управління ПК можна встановити кібербезпековий інструмент, що працює на основі браузерних плагінів, для моніторингу використання некорпоративних облікових записів.

10. Впровадження КСЗІ в даний час взагалі має якийсь сенс?

Так, впровадження КСЗІ важливе для українських державних установ та критичних об'єктів. Це мінімальний стандарт, який допомагає забезпечити базовий рівень захисту. Однак, комерційним структурам варто орієнтуватися на додаткові стандарти, як-от ISO 27001 або NIST, для більш гнучкого та комплексного захисту.

11. Чи є різниця кіберзахисту малого і середнього бізнесу та кіберзахисту військової частини? І в чому саме полягає ця різниця, якщо вона є?

Основна різниця полягає в пріоритетах і рівні загроз. Військові частини зіштовхуються з більш складними та цілеспрямованими загрозами, тому їхні системи мають бути більш захищеними від шпигунства, саботажу та інфраструктурних атак. Однак принципи розбудови кібербезпеки однакові.

12. Цікавить, що то за засіб, який може моніторити всю систему, приблизно 150 комп'ютерів, 20+ серверів, 100+ користувачів ?

Це дуже важливе питання, і ми детальніше обговоримо його на наступних лекціях. Для моніторингу інфраструктури та управління кібербезпекою варто використовувати комплексний підхід із різними інструментами, які охоплюють як мінімум:

- Централізоване управління комп'ютерами та конфігураціями (наприклад, через Active Directory або інші LDAP рішення).
- Управління обліковими записами користувачів (як локальними, так і SaaS) за допомогою Identity and Access Management (IAM) систем.
- Використання рішень для виявлення та реагування на загрози (Endpoint Detection and Response - EDR, Antivirus, Antimalware).
- Платформа для проведення регулярних тренінгів для співробітників з основ кібергігієни та обізнаності щодо загроз.
- Управління вразливостями, моніторинг оновлень, а також регулярне встановлення патчів для захисту від відомих вразливостей.

13. Хто такі кіберпанки?

Кіберпанки — це жанр наукової фантастики, що виник у 1980-х роках і зосереджується на поєднанні високих технологій з антиутопічними, соціальними та політичними темами. Підкреслюється вплив технологій на суспільство, особливо на фоні швидкого розвитку інформаційних технологій та корпоративного контролю. Наразі це своєрідна культурна та соціальна течія.