Сесія запитань та відповідей. Тренінг №2

1. Чи можна використовувати відкритий код (open-source) для побудови системи кіберзахисту? Які переваги та ризики пов'язані з такими рішеннями?

Звісно, краще використовувати вендорське рішення, оскільки ви отримуєте підтримку від розробника, але й open-source для цієї задачі може бути використаний (хоча він і не може повною мірою закрити всі потреби). З переваг - це, звісно, відсутність вкладення коштів, легкість адаптації під власні потреби, серед ризиків дуже критичною є сама суть open-source - цей код доступний і для зловмисників (для дослідження, доповнення зловмисними імплантами)

2. Які є підходи до побудови стратегії безперервного моніторингу безпеки?

Як і було сказано на тренінгу - SIEM для збору та аналізу безпекових подій, IDS/IPS для швидкого та ефективного виявлення і запобігання проникненню, моніторинг логів, поведінковий аналіз систем та користувачів, сканування систем на наявність вразливостей, контроль мережевого трафіку, автоматизація для пришвидшення реагування

3. Як ви оцінюєте ефективність таких технологій, як квантова криптографія, у контексті довгострокового кіберзахисту для глобальних хмарних сервісів? Які виклики виникають при інтеграції таких технологій?

Квантові технології в цілому - це великий прорив і висока ефективність, але вони досі є дуже вартісними та складними для розгортання, знову ж - стандарти для цих технологій ще не існують. Щодо викликів - нікуди не зникають класичні виклики хмарних технологій і до них додаються ще й описані раніше.

4. Які є формули для розрахунку ризику з точки зору кібербезпеки, як вираховуються коефіцієнти ваги критеріїв ?

Є базова формула ризику: ризик=ймовірність загрози * вплив загрози, але існує і її розширена версія: ризик=ймовірність загрози * вразливість * вплив загрози

Щодо коефіцієнта ваги критеріїв, можна обрати один зі способів визначенні ваги - експертний підхід з урахуванням контексту, на основі ретроспективи минулих інцидентів для конкретної організації, метод аналізу ієрархій (парне порівняння критеріїв після опитування або оцінювання), використання машинного навчання (урахування ретроспективи та великих масивів даних). У підсумку формула розрахунку ризиків матиме такий вигляд:

$$Ризик=W1\times Ймовірність+W2\times Вразливість+W3\times Вплив$$

де W - вага для кожного з критеріїв

5. Які основні нормативні документи регулюють кіберзахист в Україні та світі?

Для світу це ISO27001, CIS Controls (про нього більше буде у 4-му тренінгу), USA - NIST CSF, Critical Infrastructure Protection Act, Cybersecurity Act of 2015, Europe - NIS2, GDPR, ENISA, Україна - Закон України "Про основні засади забезпечення кібербезпеки України" (2017), Закон України "Про захист інформації в інформаційно-комунікаційних системах", Концепція розвитку системи кібербезпеки України, Закон України "Про захист персональних даних"

6. Розкажіть, будь ласка, про модель порушника? Чи доцільно її використовувати?

Якщо ми говоримо про модель поведінки порушника (зловмисника), то її використання буде корисним з метою розуміння кроків, які виконує зловмисник з метою отримання чутливих даних, впливу на роботу інфраструктури - ця модель дуже детально розписана як ланцюжок кібервбиства (Cyber Kill Chain). В цілому, у такий спосіб ми розуміємо, на якому етапі своїх дій знаходиться зловмисник, відповідно можемо планувати захисні дії з метою зупинки і викорінення зловмисної діяльності.

7. Який мінімальний прайс на аудит системи КБ захисту?
Це предмет обговорення замовника з виконавцем.

8. На жаль поки що розумію, що з погляду власника малого та супер-малого бізнесу, який не розбирається в кібербез, є два рівні підходу: або звернутись до кваліфікованого спеціаліста з cybersecurity щоб перекласти відповідальність, або поставити щось дуже просте як то антивірус та не клікати на фішингові лінки.

Тут не зовсім про перекладення відповідальності, тут, скоріше про залучення професіонала, який забезпечить захист бізнесу і його активів. Щодо “клікання лінків” - розмір бізнесу тут неважливий, оскільки підвищення обізнаності співробітників це мінімальна потреба будь-якого бізнесу.

9. Нажаль не почув проміжного варіанту, щоб бюджет не просів, але найбільш часті вразливості закрити.

Про це розповідалось тренінгу - тут може допомогти використання автоматизованого інструменту сканування на вразливості.

10. Малий бізнес не завжди може собі дозволити замовити пентестинг. Чи є ресурси для навчання саме в такому випадку? Не сертифікати отримувати, а ознайомлюватись та втілювати поступово?

Щодо навчання, а не сертифікацій - тут варто розрізняти: навчання, це про отримання знань і їх використання, сертифікація - це про підтвердження цих самих знань і існуючих навичок. Ресурсів для навчання (навіть безкоштовного) більш ніж достатньо, ось деякі з

них - skillsforall.com (для розвитку з нуля), HackTheBox, TryHackMe, BlueTeamLabsOnline - для отримання практичних навичок за різними напрямками у кібербезпеці.

Мається на увазі, що для будь-якого бізнесу окрім як безпосередньо в cybersecurity, цей напрямок діяльності є другорядним, не головним. Гроші приносить саме основний напрямок діяльності. Попросту не вистачає часу самостійно розбиратись в тонкощах.

Так, звісно, пентест є для малого бізнесу дуже "важким" у фінансовому плані, погоджуюсь. Розумію, що кібербезпека то є додаткове бюджетування, якого хочеться уникати, бо воно не про заробіток, а про захист головного процесу заробітку. Тут все просто: якщо ви підтримуєте власний імунітет (нормально і правильно харчуєтесь, отримуєте вітаміни, на що витрачаєте кошти), то вірогідність захворювання буде дуже низькою, якщо ж навпаки - ця вірогідність тільки росте, аналогічно і в бізнесі - якщо бізнес росте, приносить заробіток, то виникає питання репутації, довіри, відповідно для цих питань потрібне забезпечення захисту і додаткових витрат.

11. Було б цікаво почути відповідь на питання: Як система кіберзахисту верифікаційних запитів через API може виявляти та запобігати атакам, пов'язаним з автоматизованим склікуванням SMS під час відправлення коду верифікації, коли зловмисник використовує скрипт для емулювання поведінки користувача? Цей скрипт постійно підбирає комбінації номерів телефонів, IP-адрес та User-Agent'ів. Які методи та інструменти застосовуються для ідентифікації таких автоматизованих запитів та як можна обмежити або блокувати їх?

Дякую за цікаве і досить глибоке питання. Система кіберзахисту повинна використовувати комплексний підхід, що поєднує декілька рівнів захисту, таких як рейт-лімітинг, CAPTCHA, поведінковий аналіз, токенізація та інші методи, щоб ефективно виявляти та блокувати атаки на верифікаційні запити через API, зокрема атаки з автоматизованим склікуванням SMS-кодів.

12. Треба користуватись пароль-менеджером, бажано імейл аліасами і т.д.

Якщо я правильно зрозумів, то це питання/ремарка, стосується продемонстрованого інструменту HaveIbeenPwned.

Щодо тих засобів, які ви вказали - я не маю довіри до пароль-менеджеру, який самостійно а) невідомо де зберігає паролі окрім браузеру, б) без мого дозволу перевіряє їх (як передає, де саме, чи зберігаються вони на цьому шляху і т.і.), в) невідомо кому повідомляє про "безпечність" моїх паролів.

Щодо HaveIbeenPwned - це, загальнодоступний інструмент перевірки можливих витоків данних (конкретно, імейлу) на різних ресурсах, який підкаже - чи варто перейматись про безпеку і безпечність власної електронної скриньки. Але дякую за вашу думку.