Побудова ефективної функції інформаційної безпеки та Security Operations Centers як частина системи внутрішнього контролю

Київ,

Жовтень 2019

Олексій Янковський

— Партнер KPMG, Керівник групи консультування з IT та Кібербезпеки, Віце-президент ГО “ICAKA Київ”

— Практичний досвід організації реагування на масштабні кібератаки, розбудови функції та стратегії IT та Кібербезпеки

— Проведення тренінгів з реагування для низки державних та приватних організацій

— 20+ років в сфері IT та Кібербезпеки, з них 10 років в консалтингу

— CIO великої фінансово-промислової групи (промисловість, медіа, банківський бізнес)

— Barclays, ING, SAIC, George Mason University

— Міжнародні професійні сертифікати з Управління Інформаційною Безпекою, Кібербезпеки, та управління корпоративними IT (CISM, CSX Fundamentals, CGEIT)

+38 050 315 7995

ayankovski@kpmg.ua

Порядок денний

1. Глобальні втрати та виклики
   Що ми бачимо під час аудиту?

2. Глобальні тренди

3. Підходи до побудови ефективної організації
   Принципи побудови ефективних команд
   Показники ефективності

4. Security Operations Center

— Визначення
— Переваги від створення
— Варіанти структури
— Технічні засоби
— Впровадження

5. Інструменти, тренінги та сертифікації

6. Висновки

Основні виклики в сфері інформаційної безпеки

Дігіталізація – підвищення залежності бізнесу від IT

Нові технології що вимагають нових інструментів захисту (cloud, BYOD, віддалена робота, перенос периметру на endpoint та ін.)

Кіберзагрози

Геополітичні загрози

Нестача кваліфікованих ресурсів

Регуляторні вимоги (GDPR, та ін.)

Втрати від кібератак в глобальному масштабі

Атаки впливають на фізичні процеси, людське життя, існування організацій, довкілля та національні економіки.

- Глобальні втрати від кіберзлочинності в 2016 - $450 млрд. дол. США
- WannaCry (2017) – $8 млрд. дол. США
- Середні втрати від кіберзлочинності серед компаній – 7-11 млн. дол. США, досягають 74 млн. дол. США (дослідження Ponemim Institute)

Прогноз Lloyds (страховий ринок Лондона) – найближчим часом на нас чекає кібератака, втрати від якої сягнуть $53 млрд. дол. США.

Наслідки деяких атак будуть катастрофічними

Що ми бачимо в Україні

Функція ІБ слабо представлена на рівні керівництва

Ігнорування вимог служб ІБ

Недостатня кількість персоналу та незріла структура (відділ/сектор кібербезпеки із 2-3х співробітників)

Низький рівень взаємодії функцій ІТ та ІБ

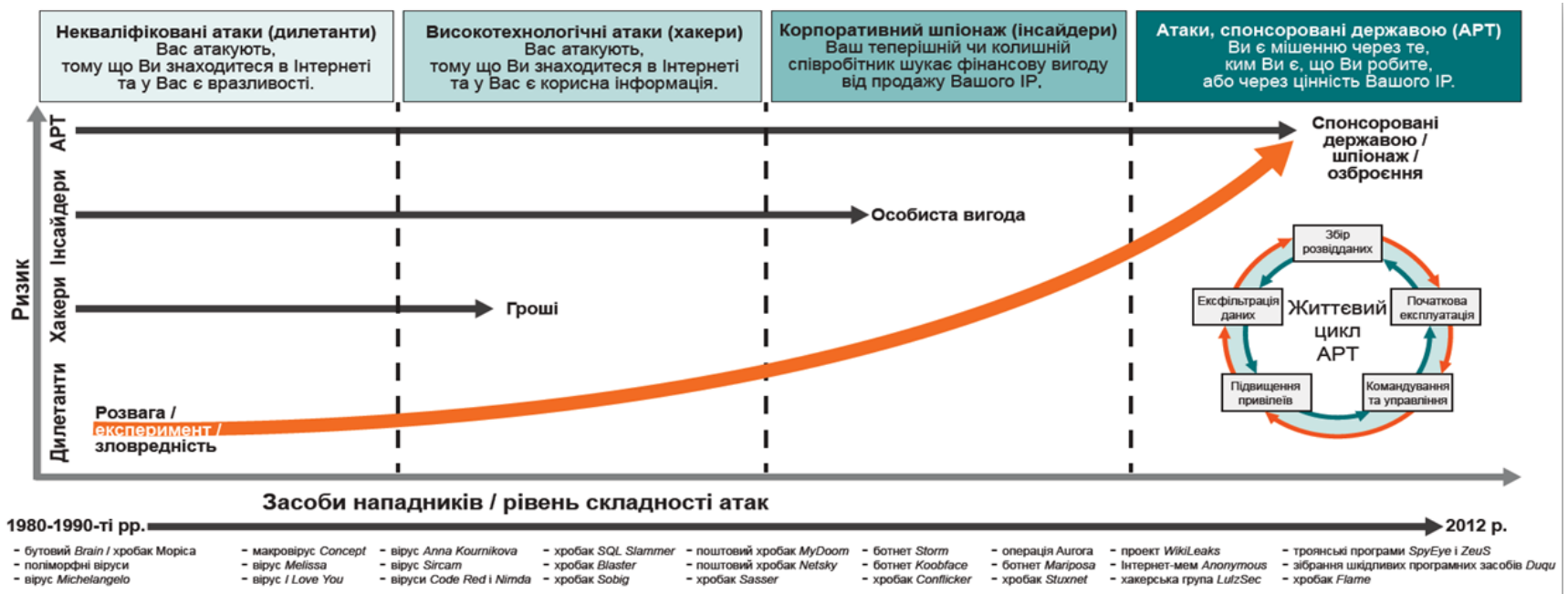
Недостатній рівень компетенції

Україна — полігон для випробування нових інструментів та кіберзброї

Менеджмент та власники великих компаній відчувають стурбованість, але не розуміють ризиків, не знають підходів та не мають інструментів

Рівень загроз суттєво збільшився

Зловмисники мають необмежений час та величезні ресурси



Джерело: *Реагування на цільові кібератаки*, ISACA, США, 2013 р., малюнок 2.

Advanced Persistent Threat – складна, спрямована, постійно-діюча загроза. Чисельні організовані злочинні угруповання, кожне з яких має кваліфіковану команду з широким набором різнопланових компетенцій та необмежені ресурси. Часто спонсовані державами.

Зміна парадигми

Вплив на організації

- Фокус не тільки на запобігання, але й на реагування – виявлення вторгнень та відновлення
- Реформування (розбудова) функцій інформаційної безпеки в організаціях, а також розвиток нових навичок
- Побудова бізнес-процесів та методів захисту із розумінням того, що системи компанії вже було скомпрометовано
- Постійна зміна системи захисту у відповідності до нових ризиків та загроз («адаптивна кібербезпека»)
- Використання нових інструментів – Кіберстрахування

Кожну організацію рано чи пізно буде зламано!

Глобальні тренди (1/3)

Зміна пріоритетів, які стоять перед функцією ІБ

— Захист життя людей, довкілля, стабільної роботи (існування) організації
— Фокус на реагування та відновлення
— Не тільки захист інформації, але й IT-залежних процесів та виробництва

Організаційні зміни

— Посилення ролі ІБ в організаціях
— Реорганізація та централізація служб ІБ
— Функціональна спеціалізація
— Впровадження централізованих Security Operations Centers (SOC) у великих компаніях (в т.ч. інтегрованих з NOC, центрами захисту АСУТП, фізичної безпеки)
— Дотаткові навички, навчання та механізми мотивації для ІБ
— Аутсорсинг окремих задач чи всієї функції

Глобальні тренди (2/3)

Створення, або посилення процесів

- Проведення симуляцій вторгнення (Red-Team/Blue-Team Exercise)
- Управління інцидентами та безперервною діяльністю
- Моніторинг подій безпеки
- Кібер-розвідка (Threat Intelligence) та обмін з галузевими центрами (Information Sharing & Analysis Centers)
- Захист систем управління технологічними процесами
- Навчання користувачів, топ-менеджменту та технічних спеціалістів
- Управління вразливостями та врпрвадження Adaptive Cybersecurity Lifecycle
- Безпека ланцюга поставок (включаючи розробку ПЗ), DevSecOps
- Цифрова криміналістика
- Розслідування, Forensics
- Страхування кібер-ризиків

Глобальні тренди (3/3)

Архітектура і технології

— Defence-in-depth (багаторівневий захист)

— Сегментація та компартменталізація

— Технології роботи з даними для виявлення вторгнень та збагачення інформації - Behavioral Analytics, Machine Learning, Big Data, Data Enrichment

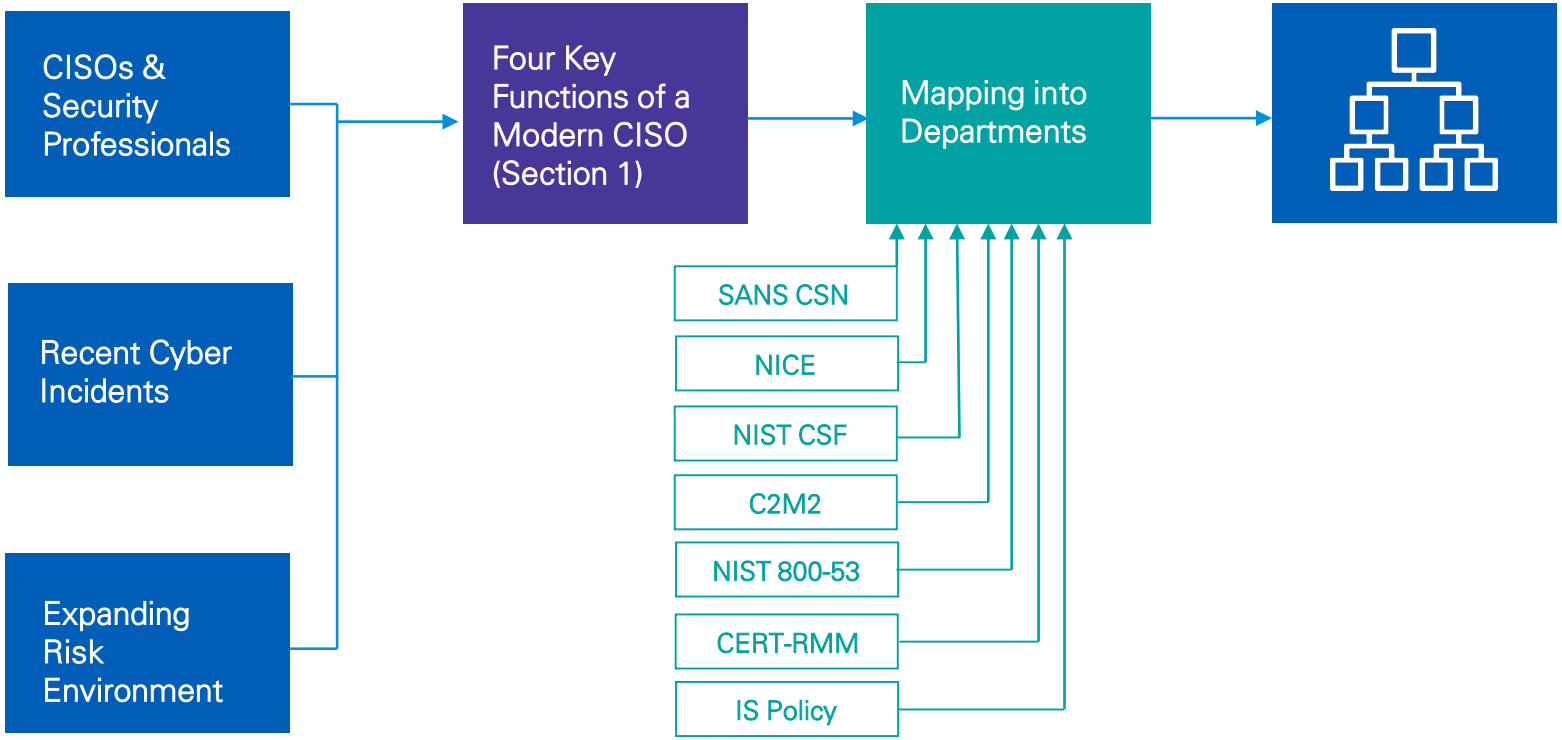
— Рішення для захисту інформації в хмарах

— Посилена автентифікація

— Open-source ПЗ

Чим має займатись функція ІБ в організації

Дослідження університету Карнегі-Мелона



Модель Карнегі-Мелона

Ключові напрямки діяльності

1. Управління, організація, політики, забезпечення виконання регуляторних вимог, управління ризиками ІБ
2. Захист і запобігання інцидентам ІБ
3. Моніторинг, та виявлення інцидентів
4. Реагування та відновлення

Принципи роботи

Збалансованість ризиків та вартості заходів безпеки

Достатній рівень моніторингу подій

Операційний контроль найбільш критичних напрямків

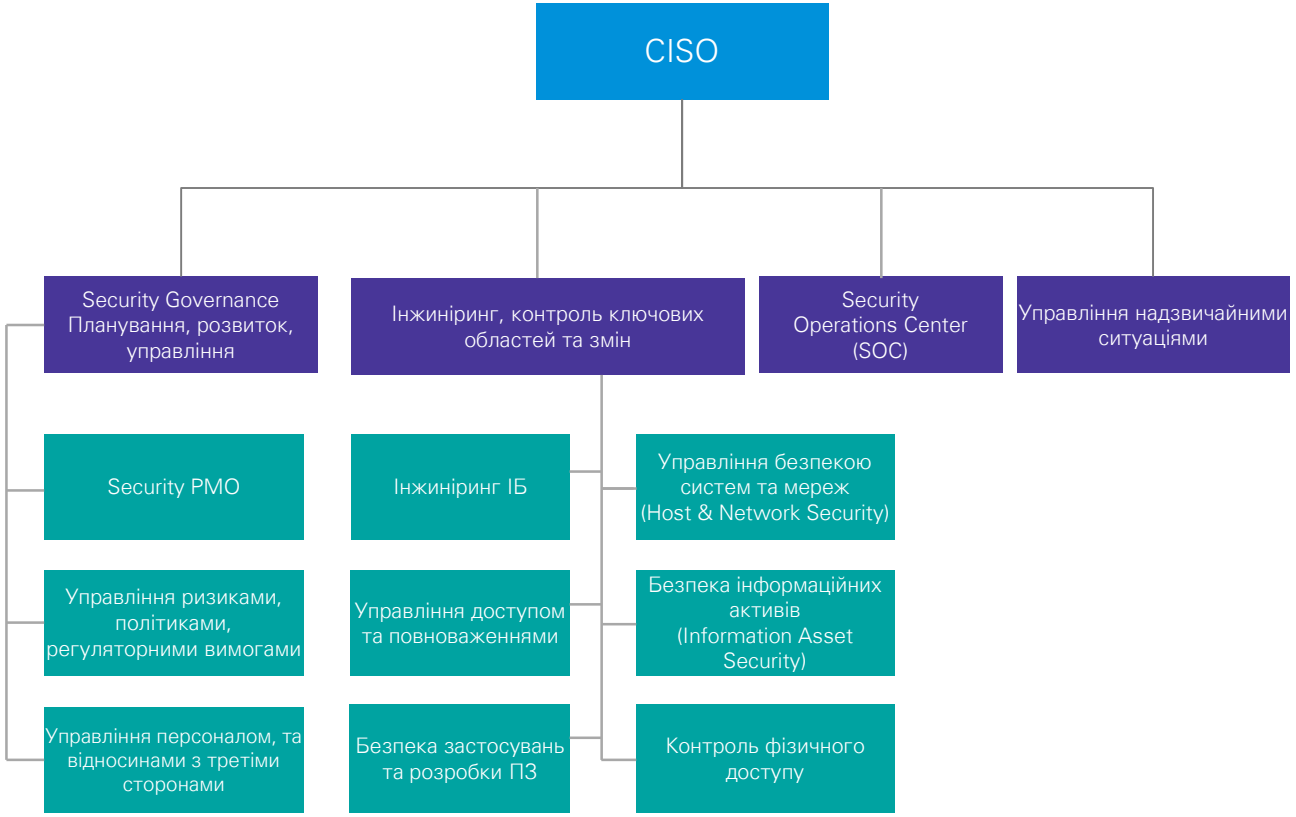
Відділення управлінських, інженерних та операційних задач

Функціональна спеціалізація

Діалог з бізнесом та створення цінності

Командний дух та партнерські стосунки з IT та іншими функціями

ЕТАЛОННА організаційна структура ІБ згідно моделі Карнегі-Мелона



Для оцінки кількості персоналу функції ІБ рекомендовано використовувати галузеві бенчмарки (Gartner, Forrester, Computer Economics та ін.) - % Security FTE від IT FTE, Загальної кількості персоналу, кількості пристроїв тощо

Висновки

1. Кібербезпека – питання для топ-менеджменту та наглядових рад

2. Організації повинні розбудовувати повноцінну функцію Інформаційної Безпеки та навчати персонал для протистояння новим викликам

3. Необхідна узгоджена та зрозуміла стратегія розвитку

4. Необхідно впроваджувати адаптивну (ризик-орієнтовану) модель захисту, яка забезпечить оперативне внесення змін в архітектуру та процеси, відштовхуючись від нових загроз

5. Бізнес-процеси та захист необхідно будувати виходячи з того, що зловмисники вже всередині

6. Існують інструменти та настанови, які можуть допомогти у впровадженні

kpmg.ua