Киберсигурност и устойчив бизнес, СИ

Конспект

доц. д-р Георги Шарков,
гл. ас. Д-р Мая Стоева

02 Април, 2024

Теми

1. Цифрова трансформация, дигитализация и киберсигурност. Цифрова зависимост и свързани оперативни рискове. Кибер терен (кибер пространство) и свързани рискове. (уводната презентация, Part 1)
2. Оперативни рискове и управление на устойчивостта и надеждността на ИТ-базирани (дигитализирани) системи и услуги. Компоненти за оценка на риска. Тенденции за увеличаване на рисковете (глобализация, дигитална зависимост....). Преглед на дейностите, моделите и стандартите за информационна сигурност и надеждност на ИТ (компютърни и мрежови) ресурси. (увод от Part 2).

3. Модел CERT-RMM. Източници, предназначение и внедряващи организации. Обща структура. Основни категории процеси, базови активи (assets), класификация на слабостите и заплахите.

4. Детайлно описание на активите и ресурсите, свързани с технологични (компютърни и мрежови) и информационни ресурси. Одит (оценка) на заплахите и слабостите, отговорности и устойчивостта на ресурсите. Стратегии и планове за Protect и Sustain (на операции, активи).
5. Триадата за информационна сигурност КИН (Конфиденциалност, Интегритет, Наличност); CIA (Confidentiality, Integrity, Availability). Прилагане и за другите базови активи (хора, технологии, инфраструктура). Видове мерки за защита (protect) и осигуряване на устойчивост (sustan) на информационни активи (Part 2, Assets, домашното/упражнение).

6. Избрано от процесни области: Engineering category, RTSE - Resilient Technical Solution Engineering - Secure coding principles. Zero Trust Architectures.
7. Избрано от процесни области: Operations management: ID – Identity Management; Access Control. Authentication, authorization, multi-factor authentication. (Part 2, допълнителна презентация за Authentication, Authorization, Access control).
8. Избрано от процесни области: Operations management: IMC – Incident Management and Control. SIEM (Security Information and Event Management), SOC (Security Operations Center), Оперативни процедури за ескалация и отговор на инциденти.
9. Анатомия на модерните атаки (уеб, мобилни). Cyber Kill Chain (основен модел, отделни фази) - уводната част от Part 2. Социално инженерство - цели, подходи.

10. Изготвяне и представяне на доклад (презентация) за заплахи, слабости, кибер атаки. Оценка на щетите. Превенция и реакция