Киберсигурност и устойчив бизнес, СИ

Конспект

гл. ас. д-р Шарков,
гл. ас. Д-р Мая Стоева
18 Март, 2022

Теми

1. Оперативни рискове и управление на устойчивостта и надеждността на ИТ-базирани (дигитализирани) системи и услуги. Преглед на моделите и стандартите за информационна сигурност и надеждност на ИТ (компютърни и мрежови) ресурси.

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

3. 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. Удовлетворяване на принципите за CIA (Confidentiality, Integrity, Availability).

4. Избрано от процесни области:
   Engineering category, Operations category.
   Детайлно представяне и упражнения за:
   - ADM - Asset Definition and Management
   - RRD - Resilience Requirements Development
   - RTSE - Resilient Technical Solution Engineering
   - SC – Service Continuity
   - AM – Access Management
   - ID – Identity Management
   - IMC – Incident Management and Control
   - PM – People Management
   - TM – Technology Management
   - VAR – Vulnerability Analysis and Resolution

5. Анатомия на модерните атаки (уеб, мобилни). Примери.
   Разглеждане на log-файлове за трафик, средства (WireShark, др.)
   Оценка на риска (слабости, уязвимости, exploits), дизайн и интеграция с cloud-базирани услуги (информация, защита, криптиране).
   Рискове и специфични политики при използване на лични устройства в организацията (BYOD = Bring Your Own Device).

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