Тема 10

Физическа сигурност

Увод

- Традиционно физическата сигурност не се свързва с информационните технологии, но тъй като организациите все по-често заменят хартията и ръчните методи на обработка на информацията с помощта на ИТ, то физическата сигурност **засяга** силно и модерните методи на съхранение и обработка на информацията.
- Физическата сигурност се занимава със защитата на **физическите активи** на една организация. Тези активи могат да бъдат: компютърна техника, мрежово оборудване, комуникационно оборудване, хардуер за съхранение на данни, документи или други технически средства.
- Обект на внимание е и сигурността на **хората(потребителите**)

. . .

- Заплахите за информацията могат да дойдат от различни посоки.
- Да вземем например малка фирма, която работи с няколко КС не използва мрежови ресурси за архивиране, а разчита на архиви правени през няколко дни. Ако някой служител неволно разсипе някаква напитка върху КС и тя дефектира е възможно част от ценна информация да се загуби.
- Друга ситуация може да бъде предизвикване по невнимание на пожар, при който да бъдат засегнати хора и унищожени КС, архиви, вкл. на хартия, и др.
- Други ситуации могат да бъдат: токови удари, кражба, екстремно високи или ниски температури и мн. др.
- Такива ситуации са обект на физическата сигурност, защото се засяга физическото съществуване на информацията, потребителите или работата на Инф. системи.

Какво е физическа сигурност?

(1) Система от политики, процедури, мерки, средства и способи за защита на персонала, инфраструктурата, собствеността и информацията на ниво организация.

(2) Физическа сигурност е защитата на персонала, хардуера, програмите, мрежи, както и данни от физически обстоятелства и събития, които биха могли да причинят сериозни загуби или вреди на една организация.

Основни характеристики на физическата сигурност (ФС)

- Неделима част от другите видове сигурност
- Струва пари
- Проблем в един елемент води до проблем в цялата система за сигурност
- Динамична
- Човешки фактор
- Непредвидима

Управление на ФС

- Както и останалите аспекти на ИС разглеждани до момента и ФС трябва да бъде обект на управление, регулации, отговорности, организация и т.н.
- ФС трябва да бъде част от програмата за информационна сигурност.
- Тъй като засяга и персонала трябва да бъде съобразена и със законодателството, напр. НАРЕДБА № Із-2377 ЗА ПРАВИЛАТА И НОРМИТЕ ЗА ПОЖАРНА БЕЗОПАСНОСТ ПРИ ЕКСПЛОАТАЦИЯ НА ОБЕКТИТЕ, издадена от Министерството на вътрешните работи.
- Необходима е адекватна управленска структура (мениджмънт), например:

➢ на високо ниво с общи отговорности за политиките по ФС, физ. охрана, безопасни условия на труд, пожарната безопасност и др.

➢ ИТ мениджъри с отговорности за напр. достъп до сървърни помещения, елзахранване на системите, температурни и влажностни условия за техниката и др.

➢ Мениджъри по ИС с отговорности напр. за нанализ на риска, мониторинг, разпределение на дневните задачи и др. не засегнати в горните две категории

Политика по Физическа сигурност

- Отговаряща на минималните стандарти за сигурност
- С включване на висшето ръководство по периодични прегледи и мониторинг
- Определена от критичността на активите и тяхната стойност
- Включваща ограничен достъп само за определен персонал
- Идентификация на персонала и посетителите

Политика по Физическа сигурност

- Специални процедури за сигурност
- Точно определени функции на мениджъра по сигурността
- Система за докладване на инциденти
- Правила за работа с класифицирана информация
- Контрол на доставките
- Зони за сигурност
- Анализ на текущата информация

Активи обект на физическа защита

- **Хардуер** – терминали, сървъри, принтери, скенери, мрежово оборудване, твърди и оптични дискове и др.
- **Софтуер**
- **Хора**, в т.ч. Персонал
  Клиенти
  Доставчици
  Посетители
- **Сгради**
- **Съоръжения**

. . .

- **Инфраструктура**
- **Репутация, имидж**
- **Данни (информация)** – на информационен носител, Интернет хранилище или резервни копия
- **Документи –** договори, чертежи, патенти, разпореждания, архив …
- **Друга собственост на организацията**

Видове заплахи за физическата сигурност

Природни

- Лошо време – бурен вятър, проливен дъжд, студ и жега
- Земетресения
- Урагани
- Цунами
- Градушки
- Сняг
- Свлачища
- Наводнения
- Пожари
- Епидемии
- Светкавици

Индустриални

- Обгазяване, задимяване
- Химикали, отрови
- Срутвания
- Опасна работна среда
- Радиация
- Спиране на електрозахранването, водата, телефони, отопление
- Проблеми с охлаждане/загряване

Социални

- Бунтове, блокади
- Стачки и протести
- Насилие на работното място, вкл. сексуално
- Организирана престъпност
- Корупция и рекет
- Атентати

Военно- политически, етнически и религиозни

- Война
- Въоръжени конфликти
- Бежанци
- Шпионаж

Заплахи, свързани с използването на компютърни, информационни и комуникационни технологии

- Вируси
- Троянски коне
- Интернет атаки
- Спам
- Сривове в системата – Интернет, бази данни, комуникации

...

- Кражба на компютърна идентичност
- Неоторизиран достъп
- Заглушаване
- Подслушване
- Наблюдение

Човешки фактор

- Недобросъвестни клиенти и служители
- Лошо обучение, лош подбор
- Грешки в изпълнението на работните операции
- Лоша поддръжка
- Безгрижност
- Битови инциденти и заболявания
- Неспазване на процедурите за сигурност (пароли, достъп, идентификация, охрана и други)

. . .

- Кражба на идентичност или фалшива идентичност
- Кражба на квалифициран персонал
- Лош анализ и оценка на риска
- Липса на система за докладване и идентификация на заплахите
- Липса на политики и процедури
- Неадекватно поведение в резултат на употреба на лекарства, наркотици, алкохол, психични проблеми, нетрадиционно сексуално поведение, пристрастяване към хазарт, семейни проблеми и други, които дават възможност за изнудване

Физически контрол на достъпа

- Една от основните мерки за ФС
- Много важна и ефективна
- Предмет е ограничаването на достъпа до сгради и съоръжения
- Осигурява контрол върху движението на персонала в определени зони, където се намират информационните активи
- Също може да се реализира по модела на слоеве
- Използват се и технически контроли като биометрични данни и смарт карти
- Базира се на утвърдени политики, правила и процедури
- Засяга както персонала, така и посетителите

Контроли за физическа сигурност

- Т.нар. жива охрана
- Кучета
- Стени , огради, врати
- Разл. Ключалки
- ID карти и баджове
- Алармени системи
- Видеонаблюдение
- Спец. помещения напр. за изчакване, изолиране
- Водене на регистри, напр. влезли-излезли, при кого, по каква задача

Нормативна уредба

- Свързана с охраната и безопасността на труда
- Противопожарна безопасност
- Кодекс на труда
- Свързана с опазването на околната среда и водите
- Транспортни регулации
- Сеизмични изисквания
- Държавни Изисквания за защита на информацията (ЗЗКИ)
- Корпоративна политика и правила

...

- Изисквания към сградите
- Банкова сигурност – офиси, печатане на пари, анализ на риска- специална уредба
- Свързана с охранителната дейност
- Стандарти ИСО 9001-2000 и ИСО 17799
- Закон за контрол над взривните вещества, огнестрелните оръжия и боеприпасите
- Друга релевантна нормативна уредба

Мерки за физическа сигурност

Мерките, които могат да бъдат прилагани във всяка организация зависят от предмета на дейност, мащаба, региона и други фактори.

Един добър пример е Наредба 3 от ЗЗКИ, макар и да касае класифицираната информация, мерките могат да се прилагат по принцип, за да се осигури високо ниво на физическа защита.

За илюстрация ще направим кратък преглед на наредбата.

Мерки за физическа сигурност по Наредба 3

- Зони за сигурност
- Защитно осветление
- Алармена система против проникване
- Контрол на физическия достъп
- Защита срещу подслушване, осъществявана с или без технически средства
- Защита срещу неправомерно визуално наблюдение
- Осъществяване на визуално наблюдение с или без използване на технически средства
- Сили за реагиране
- Пожарогасителна или пожароизвестителна система

Фактори които определят мерките по физическата сигурност

- Географско разположение – пътища, транспорт
- Изисквания за достъп
- Разположение на сградите
- Вътрешни пространства
- Разположение на офисите
- Възможности или необходимост от охрана
- Защита на ел. Инсталации, ВиК, парно и други инфраструктури
- Естеството на работата (по важните се защитават повече

Зони за сигурност

- По ЗЗКИ – I клас и II клас
- I клас – с пряк достъп до класифицирана (чувствителна) информация
- II клас – с непряк достъп до класифицирана (чувствителна) информация

Минимални стандарти по периметъра на зоните за сигурност

Паркиране

- Контрол на паркинга
- Контрол на близките зони за паркиране
- Указателни знаци срещу непозволено спиране
- Идентификационни процедури при паркиране - карти, пропусквателен режим и др.
- Подходящо осветление

Видеонаблюдение

- Видеозапис
- Указателни табели, посочващи че се извършва видеонаблюдение

Осветление

- Осветление с възможности за работа при авария

Физически бариери

- Бетонни или стоманени прегради
- Паркинг бариери

Минимални стандарти при влизане в зоната за сигурност

- **Изпращане приемане на пратки**
  - Контрол на пратките и куриерите
- **Контрол на достъпа**
  - Оценка на сградите и съоръженията с оглед на задълженията на охраната
  - Охранителни патрули
  - Алармена система против проникване
  - Противопожарна и пожароизвестителна система
- **Входове / изходи**
  - Апаратура за проверка на багаж, лични вещи и хора
  - Шпионки на входните врати
  - Интеркоми за връзка с посетители отвън (домофони)
  - Контрол на входа с видеонаблюдение
  - Сигурни ключалки
  - Специални стъкла – усилени, армирани, бронирани

. . .

- **Идентификация на служителите и посетителите**
  - Снимкова идентификация
  - Система за проверка и контрол на посетителите
  - Звено, което издава идентификационните карти
- **Сгради и съоръжения**
  - Предотвратяване на неоторизиран достъп до сгради и съоръжения
  - аварийно захранване на алармени системи, радиовръзки, компютри и видеонаблюдение
  - решетки и прегражданe на всички видове отвори, прозорци и входове
- **Планове за евакуация**
  - Преглед на съществуващите планове
  - Периодични учения
  - Тренировки и обучение
- **План за сигурност (физическа сигурност)**
  - На персонала и На охраната

. . .

- **Събиране на информация**
  - Връзка с полицейски и други правоохранителни органи
  - Процедури за получаване и разпространение на информация
  - Обединение и контакти с други организации
- **Защита срещу подслушване**
  - Пасивно (намаляване на електромагнитните излъчвания, криптиране на информацията, звукоизолиране в зони клас I и II)
  - Активно – техническа или физическа проверка за подслушване
- **Мерки срещу видеонаблюдение**
  - Щори, пердета, специални стъкла и други
  - Осигуряване на технически защитени зони срещу подслушване и наблюдение

Практически упражнения

- В рамките на един учебен час потърсете в Интернет пространството информация за разглежданите в темата понятия, дефиниции и аспекти. Търсенето може да направите и на чужди езици, които владеете.
- Анализирайте намерената информация и я сравнете с поднесената тук.
- Проучете какви мерки за физическа сигурност се прилагат в позната Ви организация.
- Набележете мерки за физическа сигурност на информацията в личен план.