НАРЪЧНИК

ИНФОРМАЦИОННА СИГУРНОСТ ЗА НПО

ПО-ДОБРО РАЗБИРАНЕ НА **КИБЕР РИСКОВЕТЕ** И ПРАКТИЧНИ ИНСТРУМЕНТИ ЗА **НАДЕЖДНА ЗАЩИТА В ИНТЕРНЕТ**

STARTUPFACTORY.BG

2024

ИНФОРМАЦИОННА СИГУРНОСТ ЗА НПО

Тази електронна книга предоставя на служителите в НПО сектора в България необходимата информация за по-добро разбиране на кибер рисковете, както и практични инструменти за надеждна защита в Интернет.

Електронната книга е създадена от екипа на сдружение **Startup Factory** в рамките на проект **InfoSec Skills+**, който се реализира с финансовата подкрепа на **Transatlantic Foundation** по проект **PROTEUS**, съфинансиран от **Европейския съюз**. Изявленията и мненията, изразени тук, принадлежат единствено на сдруже-ние **Startup Factory** и не отразяват непременно вижданията на Европейския съюз или Европейската изпълнителна агенция по образование и култура. Европейският съюз и представля-ващият орган не могат да носят отговорност за тях.

STARTUP FACTORY

Финансирано от Европейския съюз

G | M | F Transatlantic Foundation

2024

СЪДЪРЖАНИЕ

2024

СЪДЪРЖАНИЕ

2024

СЪДЪРЖАНИЕ

Глава 1

Въведение в информационната сигурност

1.1 ЗНАЧЕНИЕ НА ИНФОРМАЦИОННАТА СИГУРНОСТ В НПО ОРГАНИЗАЦИИТЕ

Информационната сигурност е изключително важна за НПО организациите, защото те често **обработват чувствителни данни за своите донори, бенефициенти и партньори**. Загубата или компрометирането на тази информация може да доведе до сериозни последици, включително загуба на доверие, финансови загуби и юридически последствия.

Примери за чувствителна информация в НПО:

- Лични данни на бенефициенти и донори
- Финансови документи и отчети
- Данни и резултати от проекти
- Комуникация и кореспонденция

1.2 ОСНОВНИ ТЕРМИНИ И ПОНЯТИЯ

Информационна сигурност:

Практиката за защита на информацията от неразрешен достъп, използване, разкриване, разрушаване, модифициране или разрушаване.

Заплахи:

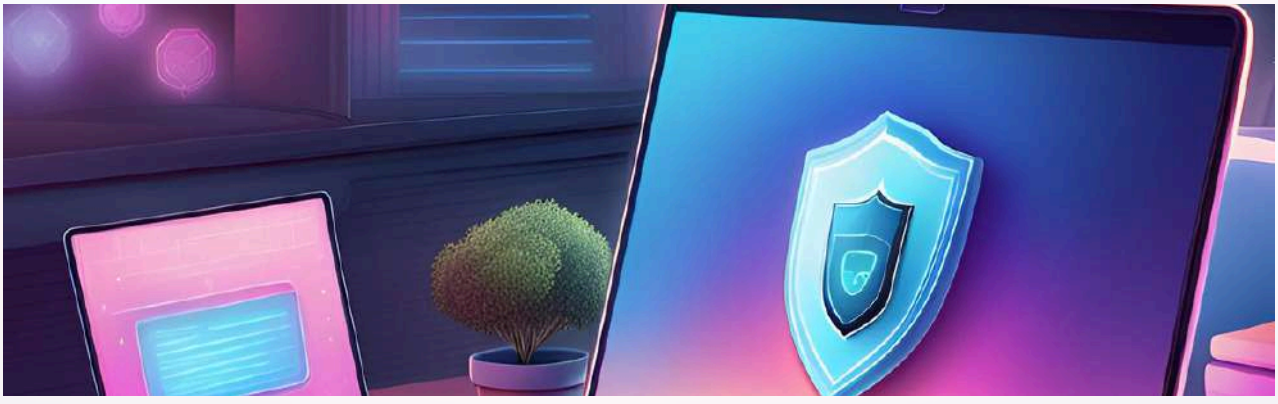
Всяко потенциално събитие или действие, което може да причини щети на информационните системи или данни.

Уязвимости:

Слабости в системите или процесите, които могат да бъдат експлоатирани от заплахи за причиняване на щети.

Рискове:

Вероятността заплаха да експлоатира уязвимост и въздействието, което това може да има върху организацията.



1.3 ПРЕГЛЕД НА ЗАПЛАХИТЕ И РИСКОВЕТЕ

Често срещани заплахи за НПО:

Фишинг атаки: Измамни съобщения, целящи да подмамят служителите да разкрият конфиденциална информация или да инсталират зловреден софтуер.

Зловреден софтуер: Програми, които могат да повредят или компрометират информационните системи.

Неоторизиран достъп: Достъп до системи или данни без разрешение.

Изтичане на данни: Непреднамерено разкриване на чувствителна информация.

Примери за уязвимости в НПО:

Слаби пароли: Използване на лесни за отгатване или повторно използвани пароли.

Липса на актуализации: Неприлагане на най-новите актуализации и пачове на софтуера.

Недостатъчно обучение: Липса на осведоменост и обучение на служителите относно кибер заплахите.

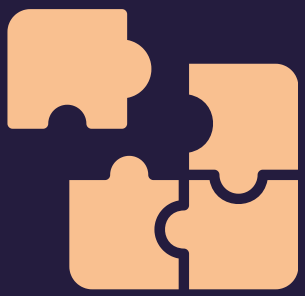
Управление на рисковете:

1. ***Идентифициране на рисковете:*** Разпознаване на потенциалните заплахи и уязвимости.
2. ***Оценка на рисковете:*** Оценка на вероятността и въздействието на заплахите.
3. ***Контрол на рисковете:*** Прилагане на мерки за намаляване на рисковете.

1.4 ПРИНЦИПИ НА КИБЕРСИГУРНОСТТА

КОНФИДЕНЦИАЛНОСТ

Защита на информацията от неразрешен достъп и разкриване.



ИНТЕГРИТЕТ

Осигуряване на точността и пълнотата на информацията и системите.

НАЛИЧНОСТ

Осигуряване на достъпността на информацията и системите, когато са необходими.

1.5 РОЛИ И ОТГОВОРНОСТИ В ИНФОРМАЦИОННАТА СИГУРНОСТ

Служители:

Отговорни за спазването на политиките и процедурите за сигурност.

Ръководство:

Осигурява ресурси и подкрепа за инициативите за информационна сигурност.

ИТ отдел или отговорник

Отговорен за внедряването и поддръжката на техническите мерки за сигурност.

Екип за реакция при инциденти:

Отговорен за откриването, управлението и разрешаването на кибер инциденти.

Глава 2

Основи на Киберсигурността

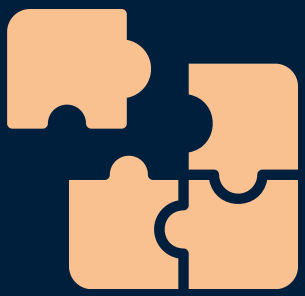
2.1 ПРИНЦИПИ НА КИБЕРСИГУРНОСТТА: КОНФИДЕНЦИАЛНОСТ, ИНТЕГРИТЕТ, НАЛИЧНОСТ

КОНФИДЕНЦИАЛНОСТ:

- ***Определение***: Конфиденциалността гарантира, че информацията е достъпна само за оторизирани лица.
- ***Примери за защита***: Използване на пароли, криптиране на данни, контрол на достъпа.

ИНТЕГРИТЕТ:

- ***Определение***: Интегритетът гарантира, че данните са точни и не са променени или повредени от неоторизирани лица.
- ***Примери за защита***: Използване на хеш функции, цифрови подписи, контрол на версиите.



НАЛИЧНОСТ:

- ***Определение***: Наличността гарантира, че информацията и ресурсите са достъпни за оторизираните потребители, когато са им необходими.
- ***Примери за защита***: Използване на резервни копия, планове за възстановяване при аварии, защита срещу DDoS атаки.

2.2 ВЪВЕДЕНИЕ В ЗАКОНОДАТЕЛСТВОТО И РЕГУЛАЦИИТЕ

GDPR (GENERAL DATA PROTECTION REGULATION):

- ***Обхват***: Европейски регламент за защита на личните данни на физическите лица.
- ***Основни изисквания***: Информирано съгласие, право на достъп, право на изтриване, уведомление за пробив на данни.
- ***Санкции***: Глобите за неспазване на GDPR могат да достигнат до **20 милиона евро** или **4% от общия годишен оборот**, което е по-голямо.

NIS-2 (DIRECTIVE ON SECURITY OF NETWORK AND INFORMATION SYSTEMS):

Това е **ревизия на Директивата за мрежите и информационните системи (NIS) от 2016 година**, която определя минимални мерки, които трябва да се предприемат, за да се **гарантира високо общо ниво на киберсигурност**.
Всички държави членки трябва да приложат NIS-2 в местното си законодателство до октомври 2024 г.

- ***Обхват***: Европейска директива за подобряване на сигурността на мрежите и информационните системи в ЕС.
- ***Основни изисквания***: Управление на рисковете, докладване на инциденти, сътрудничество между държавите членки.
- С***анкции***: Глобите за неспазване варират в зависимост от националното законодателство на всяка държава членка.

2.3 РОЛИ И ОТГОВОРНОСТИ В ИНФОРМАЦИОННАТА СИГУРНОСТ

Служители:

- ***Роля***: Спазване на политиките и процедурите за сигурност, докладване на инциденти.
- ***Отговорности***: Използване на силни пароли, предпазване от фишинг атаки, защита на устройствата.

ИТ отдел или отговорник:

- ***Роля***: Внедряване и поддръжка на техническите мерки за сигурност.
- ***Отговорности***: Администриране на мрежовите защити, актуализиране на софтуера, мониторинг на системите.

Ръководство:

- ***Роля***: Осигуряване на ресурси и подкрепа за инициативите за информационна сигурност.
- ***Отговорности***: Определяне на политики, одобряване на бюджети, наблюдение на изпълнението на мерките за сигурност.

Екип за реакция при инциденти:

- ***Роля***: Откриване, управление и разрешаване на кибер инциденти.
- ***Отговорности***: Разследване на инциденти, координиране на реакциите, комуникация с външни органи.

2.4 ВИДОВЕ ЗАПЛАХИ И УЯЗВИМОСТИ

Заплахи:

- ***Фишинг***: Измамни съобщения, целящи да подмамят потребителите да разкрият конфиденциална информация.
- ***Зловреден софтуер***: Софтуер, който може да повреди или компрометира системите.
- ***Социално инженерство***: Техники за манипулиране на хора с цел разкриване на конфиденциална информация.

Уязвимости:

- ***Слаби пароли***: Пароли, които са лесни за отгатване или се използват често.
- ***Системи без "кръпки"*** - пачове: Системи, които не са актуализирани и съдържат известни уязвимости.
- ***Липса на осведоменост:*** Непознаване на рисковете и заплахите от страна на служителите

2.5 ИНСТРУМЕНТИ И ТЕХНОЛОГИИ ЗА ЗАЩИТА

Антивирусни програми:

- Функции: Откриване и премахване на зловреден софтуер.
- Примери: Avast, Avira, Bitdefender, Norton, Kaspersky и др.

Системи за управление на пароли:

- Функции: Генериране, съхранение и управление на силни пароли.
- Примери: Google Password Manager, LastPass, 1Password, Dashlane и др.

Системи за откриване и предотвратяване на проникванията (IDS/IPS):

- Функции: Предоставят възможност за откриване и/или предотвратяване на атаки свързани с информационната сигурност, като атаки с груба сила (brute-force), атаки за отказ на услуга (DoS) и експлоатиране на уязвимости.
- Примери: Snort, Suricata и др.

2.6 ПРАКТИЧЕСКИ ПРИМЕРИ

Пример 1: Фишинг Атака

Ситуация: Служител получава имейл, който изглежда идва от банка и иска актуализация на лични данни.

Действия: Служителят докладва имейла като подозрителен. ИТ отделът анализира и блокира домейна на изпращача.

Пример 2: Зловреден Софтуер

Ситуация: Система в офиса започва да работи бавно и показва неочаквани съобщения.

Действия: Антивирусният софтуер идентифицира и премахва зловредния софтуер. Системата е възстановена от резервно копие.

Пример 3: Неоторизиран достъп

Ситуация: Открива се, че служител има достъп до данни, които не са му необходими за работата.

Действия: Преглед на правата за достъп и ограничаване на ненужните привилегии. Провеждане на обучение за служителя.

Глава 3

Политики и процедури

Глава 3

3.1 СЪЗДАВАНЕ И ПРИЛАГАНЕ НА ПОЛИТИКИ ЗА СИГУРНОСТ

ЗНАЧЕНИЕ НА ПОЛИТИКИТЕ ЗА СИГУРНОСТ:

- Политиките за сигурност са основата на ефективната защита.
- Те осигуряват насоки и правила за защита на информационните ресурси.

ПРОЦЕС НА СЪЗДАВАНЕ НА ПОЛИТИКИ:

1. Оценка на рисковете: Определяне на специфичните рискове и уязвимости в организацията.
2. Разработване на политики: Създаване на документи, които описват правилата и процедурите за сигурност.
3. Одобрение и прилагане: Получаване на одобрение от ръководството и внедряване на политиките в организацията.
4. Обучение и осведоменост: Обучаване на служителите за новите политики и процедури.
5. Регулярен преглед и актуализация: Редовно преглеждане и актуализиране на политиките според новите заплахи и промени в организацията.

3.2 ПОЛИТИКА ЗА УПРАВЛЕНИЕ НА ПАРОЛИ

ЦЕЛ:
Осигуряване на защита на потребителските акаунти чрез използване на силни и уникални пароли.

ОСНОВНИ ЕЛЕМЕНТИ:

Изисквания за дължина:
Минимална дължина на паролата от 12 символа.

Сложност:
Паролите трябва да включват главни и малки букви, цифри и специални символи.

Промяна на паролите:
Редовна смяна на паролите на всеки 90 дни или ако има и най-малките съмнения, че информацията може да е била компрометирана.

История на паролите:
Забрана за повторно използване на последните 5 пароли.

Мениджъри на пароли:
Насърчаване използването на мениджъри на пароли за съхранение и управление на паролите.

3.3 ПОЛИТИКА ЗА УПРАВЛЕНИЕ НА ДОСТЪПА

ЦЕЛ:
Осигуряване на достъп до информационните ресурси само за оторизирани потребители.

ОСНОВНИ ЕЛЕМЕНТИ:

Идентификация и автентикация:
Изискване за уникални потребителски имена и силни пароли.

Сложност:
Достъпът до системите се базира на ролите и отговорностите на потребителите (Role-Based Access Control, RBAC).

Двуфакторна автентикация (2FA):
Внедряване на 2FA за всички критични системи.

3.4 ПОЛИТИКА ЗА РЕАКЦИЯ ПРИ ИНЦИДЕНТИ

ЦЕЛ:

Осигуряване на бърза и ефективна реакция при кибер инциденти за минимизиране на щетите и възстановяване на нормалната работа.

ОСНОВНИ ЕЛЕМЕНТИ:

Екип за реакция при инциденти:
Създаване на екип, който е отговорен за управлението на инциденти.

Процедури за докладване:
Ясни процедури за докладване на инциденти.

Анализ и възстановяване:
Процедури за анализ на инциденти и възстановяване на засегнатите системи.

Докладване и превенция:
Създаване на доклади за инциденти и предприемане на мерки за предотвратяване на бъдещи инциденти.

3.5 ОБУЧЕНИЕ НА СЛУЖИТЕЛИТЕ

ЦЕЛ:
Осигуряване на знания и умения на служителите за разпознаване и предотвратяване на кибер заплахи.

ОСНОВНИ ЕЛЕМЕНТИ:

Регулярни обучения:
Провеждане на редовни обучения по киберсигурност за всички служители.

Симулации на атаки:
Провеждане на симулации на фишинг атаки и други видове заплахи..

Кампания за осведоменост:
Периодични кампании за осведомяване относно нови заплахи и добри практики.

Глава 4

Технически мерки за сигурност

4.1 ЗАЩИТНИ СТЕНИ (FIREWALLS) И АНТИВИРУСЕН СОФТУЕР

ЗАЩИТНИ СТЕНИ:

Функция: Защитните стени контролират входящия и изходящия мрежов трафик въз основа на предварително зададени правила.

ВИДОВЕ

Хардуерни защитни стени:
Обикновено са инсталирани на мрежовите граници и защитават цялата мрежа.

Софтуерни защитни стени:
Инсталират се на отделни устройства и защитават конкретното устройство.

ПРИМЕРИ ЗА НАСТРОЙКИ:

Блокиране на неоторизиран достъп
Конфигуриране на правилата за блокиране на достъпа до неразрешени IP адреси и портове.

Мониторинг и логване:
Регулярно преглеждане на логовете за подозрителна активност.

АНТИВИРУСЕН СОФТУЕР:

Функция: Антивирусният софтуер открива, блокира и премахва зловреден софтуер от компютърните системи.

ВИДОВЕ ЗАПЛАХИ:

Вируси:
Програми, които се разпространяват чрез заразяване на други файлове.

Троянски коне:
Зловредни програми, маскирани като легитимни софтуери.

Рансъмуер:
Софтуер, който криптира данни и изисква откуп за тяхното отключване.

ПРИМЕРИ ЗА АНТИВИРУСЕН СОФТУЕР:

Bitdefender:
Предлага защита в реално време и чести актуализации.

Norton:
Осигурява цялостна защита срещу различни видове зловреден софтуер.

Kaspersky:
Включва функции за откриване и премахване на зловреден софтуер и фишинг защита.

4.2 КРИПТИРАНЕ НА ДАННИ

ФУНКЦИЯ:
Криптирането защитава конфиденциалността на данните чрез преобразуването им в неразбираем формат, който може да бъде декриптиран само с подходящ ключ.

ВИДОВЕ КРИПТИРАНЕ:

Симетрично криптиране:
Един и същ ключ се използва за криптиране и декриптиране на данните.

Асиметрично криптиране:
Използва се публичен ключ за криптиране и частен ключ за декриптиране.

ПРИМЕРИ ЗА ПРИЛОЖЕНИЯ НА КРИПТИРАНЕТО:

Защита на данни при пренос:
Използване на протоколи като TLS (Transport Layer Security) за защита на данните при пренос през интернет.

Защита на данни при съхранение:
Използване на криптирани файлови системи и дискове за защита на данните, съхранявани на устройствата.

4.3 СИСТЕМИ ЗА ОТКРИВАНЕ И ПРЕДОТВРАТЯВАНЕ НА ПРОНИКВАНИЯ (IDS/IPS)

ФУНКЦИЯ:
IDS и IPS системите наблюдават мрежовия трафик и системните дейности за откриване и предотвратяване на подозрителна активност.

IDS (INTRUSION DETECTION SYSTEM):

Функция:
Открива и алармира за подозрителна активност, но не предприема автоматични действия.

Типове:

- Мрежово-базирани IDS (NIDS): Мониторинг на мрежовия трафик.
- Хост-базирани IDS (HIDS): Мониторинг на системните файлове и дейности на конкретно устройство.

IPS (INTRUSION PREVENTION SYSTEM):

Функция:
Открива и автоматично предприема действия за предотвратяване на заплахи.

Типове:

- Мрежово-базирани IPS (NIPS): Превенция на мрежово ниво.
- Хост-базирани IPS (HIPS): Превенция на системно ниво.

ПРИМЕРИ ЗА IDS/IPS СИСТЕМИ:

Snort:
Отворен код IDS/IPS система, използвана за мрежов мониторинг и откриване на заплахи.

Suricata:
Високоефективна IDS/IPS система с множество функции за анализ на мрежовия трафик.

4.4 УПРАВЛЕНИЕ НА УЯЗВИМОСТИ И АКТУАЛИЗАЦИИ

ФУНКЦИЯ:
Управлението на уязвимости включва процеси за откриване, оценка и отстраняване на уязвимости в системите и софтуера.

ПРОЦЕС НА УПРАВЛЕНИЕ НА УЯЗВИМОСТИТЕ:

Откриване: Използване на инструменти за сканиране на уязвимости като Nessus или OpenVAS.

Оценка: Оценка на откритите уязвимости въз основа на тяхната тежест и потенциален риск.

Отстраняване: Прилагане на пачове/"кръпки" и актуализации за отстраняване на уязвимостите.

Документация: Поддържане на записи за всички открити и отстранени уязвимости.

Глава 5

Управление на достъпа

Глава 5

5.1 ИДЕНТИФИКАЦИЯ И АВТЕНТИКАЦИЯ

ЦЕЛ:
Осигуряване на сигурен достъп до системите чрез проверка на идентичността на потребителите.

ОСНОВНИ ЕЛЕМЕНТИ:

Идентификация:
Всеки потребител трябва да има уникално потребителско име.

Автентикация:
Потребителите трябва да удостоверят самоличността си чрез пароли, двуфакторна автентикация (2FA) или биометрични данни.

ПРОЦЕДУРИ:

Регистрация на нови потребители: Определяне на процес за създаване на потребителски акаунти.

Управление на пароли: Настройка на минимални изисквания за дължина и сложност на паролите.

Внедряване на 2FA: Избор и конфигурация на методи за двуфакторна автентикация.

5.2 ИЗИСКВАНИЯ ЗА СИЛНИ ПАРОЛИ И УПРАВЛЕНИЕ НА ПАРОЛИ

ЦЕЛ:
Предотвратяване на неоторизиран достъп чрез използване на силни и уникални пароли.

ОСНОВНИ ИЗИСКВАНИЯ:

- Минимална дължина: Паролите трябва да бъдат най-малко 12 символа.
- Сложност: Паролите трябва да съдържат големи и малки букви, цифри и специални символи.
- Периодична промяна: Паролите трябва да се сменят на всеки 90 дни или ако има и най-малките съмнения, че информацията може да е била компрометирана.
- История на паролите: Не трябва да се използват повторно последните 5 пароли.

ПРОЦЕДУРИ:

Създаване на пароли: Инструкции за създаване на силни пароли.

Мениджъри на пароли: Обучение за използване на софтуер за управление на пароли.

Смяна на пароли: Процедури за редовна смяна на паролите и при подозрение за компрометиране.

5.3 ДВУФАКТОРНА АВТЕНТИКАЦИЯ (2FA) ЗА ВСИЧКИ КРИТИЧНИ СИСТЕМИ

ЦЕЛ:
Добавяне на допълнителен слой сигурност чрез изискване на втори фактор при удостоверяване на самоличността.

ОСНОВНИ МЕТОДИ:

Хардуерни токени:
Физически устройства, които генерират кодове за автентикация.

Софтуерни токени:
Приложения за мобилни устройства като Google Authenticator.

SMS кодове:
Кодове, изпращани като текстови съобщения.

ПРОЦЕДУРИ:

Избор на метод за 2FA: Анализ и избор на подходящи методи за двуфакторна автентикация.

Внедряване: Конфигурация и внедряване на избраните методи за 2FA.

Обучение: Обучение на потребителите за използване на двуфакторна автентикация.

5.4 УПРАВЛЕНИЕ НА ПОТРЕБИТЕЛСКИТЕ ПРАВА

ЦЕЛ:
Осигуряване на достъп до системи и данни само на оторизирани потребители.

ОСНОВНИ ПРИНЦИПИ:

Минимални привилегии:
Потребителите трябва да имат достъп само до ресурсите, необходими за тяхната работа.

Ролева база:
Управление на достъпа въз основа на роли и отговорности (Role-Based Access Control, RBAC).

ПРОЦЕДУРИ:

Дефиниране на роли: Определяне на роли и свързаните с тях права за достъп.

Преглед на правата: Редовен преглед и актуализация на правата за достъп.

Одобрение на права: Процедури за одобрение на заявки за достъп от оторизирани администратори.

5.5 ПРЕГЛЕД И ОДОБРЕНИЕ НА ДОСТЪПА ОТ АДМИНИСТРАТОР

ЦЕЛ:
Осигуряване на контрол върху достъпа чрез преглед и одобрение на всички заявки за достъп.

ОСНОВНИ ЕЛЕМЕНТИ:

Процес за заявки за достъп:
Ясно дефинирани процедури за подаване и преглед на заявки за достъп.

Одобрение:
Заявките за достъп трябва да бъдат преглеждани и одобрявани от оторизирани администратори.

Документация:
Поддържане на записи на всички одобрени и отказани заявки за достъп.

Глава 6

Защита на мрежата и устройствата

6.1 СЕГМЕНТАЦИЯ НА МРЕЖАТА

ЦЕЛ:
Разделяне на мрежата на различни сегменти за подобряване на сигурността и управление на достъпа.

ОСНОВНИ ПРИНЦИПИ:

Изолиране на критични системи:
Критичните системи трябва да бъдат изолирани от останалите части на мрежата.

Виртуални локални мрежи (VLANs):
Използване на VLANs за създаване на логически сегменти в мрежата.

ПРОЦЕДУРИ:

Анализ на мрежата: Идентифициране на критичните системи и определяне на сегментите.

Конфигурация на VLANs: Настройка на VLANs за изолиране на трафика между различните сегменти.

Мониторинг: Регулярен мониторинг на мрежовия трафик за откриване на аномалии и неоторизиран достъп.

6.2 ЗАЩИТА НА БЕЗЖИЧНИТЕ МРЕЖИ

ЦЕЛ:
Осигуряване на сигурност за безжичните мрежи, използвани в организацията.

ОСНОВНИ МЕРКИ:

Силна автентикация:
Използване на WPA3 - нов стандарт за криптиране на данни, предавани през безжична мрежа.

Скрито име на мрежата/Service Set Identifier (SSID):
Изключване на излъчването на SSID за скриване на мрежата от неоторизирани лица.

Филтриране по MAC адрес/физическия адрес на мрежовото устройство:
Ограничаване на достъпа до мрежата само за определени устройства.

6.3 ЗАЩИТА НА МОБИЛНИ УСТРОЙСТВА

ЦЕЛ:
Осигуряване на сигурност за мобилните устройства, използвани в организацията.

ОСНОВНИ МЕРКИ:

Криптиране на данни:
Криптиране на съхраняваните данни на мобилните устройства.

Управление на мобилни устройства (MDM):
Използване на MDM решения за управление и защита на мобилните устройства.

Антивирусен софтуер:
Инсталиране на антивирусен софтуер на мобилните устройства.

МОЖЕ ЛИ НЯКОЙ ДА ХАКНЕ ТЕЛЕФОНА ВИ САМО С ВАШИЯ НОМЕР?

6.5 МОНИТОРИНГ НА МРЕЖОВИЯ ТРАФИК

ЦЕЛ:
Откриване на подозрителна активност и аномалии в мрежовия трафик.

ОСНОВНИ МЕРКИ:

Инструменти за мониторинг:
Използване на инструменти като Wireshark за анализ на мрежовия трафик.

Системи за откриване на проникванията (IDS):
Внедряване на IDS системи за наблюдение и откриване на подозрителна активност.

Анализ на логовете:
Регулярен преглед и анализ на мрежовите логове за идентифициране на потенциални заплахи.

6.4 БЕЗОПАСНО ИЗПОЛЗВАНЕ НА ПУБЛИЧНИ WI-FI МРЕЖИ

ЦЕЛ:
Предотвратяване на рисковете, свързани с използването на публични Wi-Fi мрежи.

ОСНОВНИ МЕРКИ:

Използване на VPN:
Използване на виртуални частни мрежи (VPN) за защита на трафика.

Деактивиране на автоматично свързване:
Изключване на автоматичното свързване към непознати мрежи.

Ограничаване на споделянето:
Изключване на споделянето на файлове и папки при използване на публични Wi-Fi мрежи.

ОПАСНОСТИТЕ ОТ ИЗПОЛЗВАНЕТО НА ОБЩЕСТВЕН WI-FI (И КАК ДА ГИ ИЗБЕГНЕТЕ)

Глава 7

Обучение и осведоменост

Глава 7

7.1 ЗНАЧЕНИЕ НА ОБУЧЕНИЕТО ПО КИБЕРСИГУРНОСТ

ЦЕЛ: Осигуряване на знания и умения на служителите за разпознаване и предотвратяване на кибер заплахи.

ОСНОВНИ ПРИЧИНИ:

Намаляване на риска:
Обучените служители са по-малко склонни да станат жертви на фишинг атаки и други заплахи.

Подобряване на реакцията:
Служителите, които знаят как да реагират на инциденти, могат да минимизират щетите.

Спазване на регулации:
Много регулации изискват редовно обучение по киберсигурност.

7.2 ПРОГРАМИ ЗА ОБУЧЕНИЕ И ОСВЕДОМЕНОСТ

ЦЕЛ: Разработване на систематични програми за обучение, които обхващат различни аспекти на киберсигурността.

КОМПОНЕНТИ:

Въвеждащо обучение:
Основни понятия и принципи на киберсигурността за нови служители.

КУРС „ИНФОРМАЦИОННА СИГУРНОСТ ЗА НПО“ (БАЗОВО НИВО)

Редовни обновявания:
Периодични обучения за осведомяване относно нови заплахи и добри практики.

Специализирани курсове:
Обучения за специфични роли, като ИТ персонал и администратори.

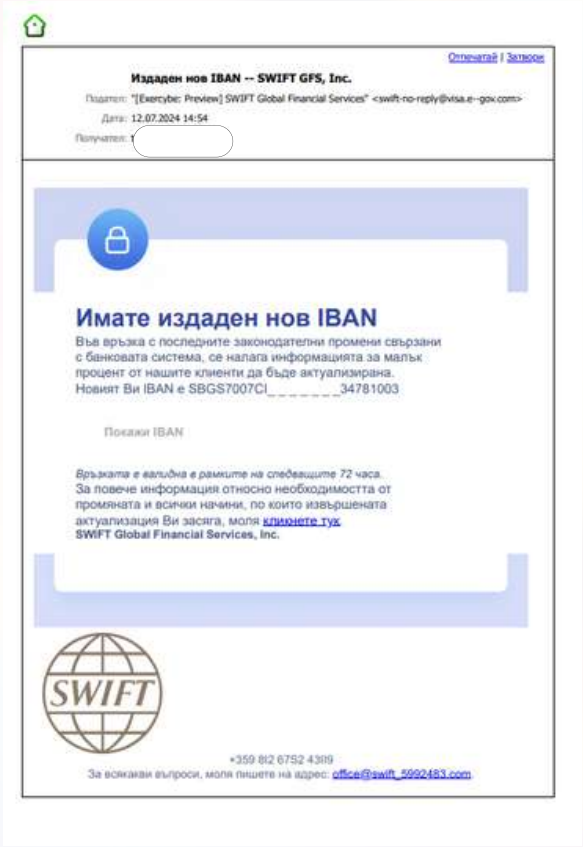
ОБУЧЕНИЕ „ИНФОРМАЦИОННА СИГУРНОСТ ЗА НПО“ (НИВО ЗА НАПРЕДНАЛИ)

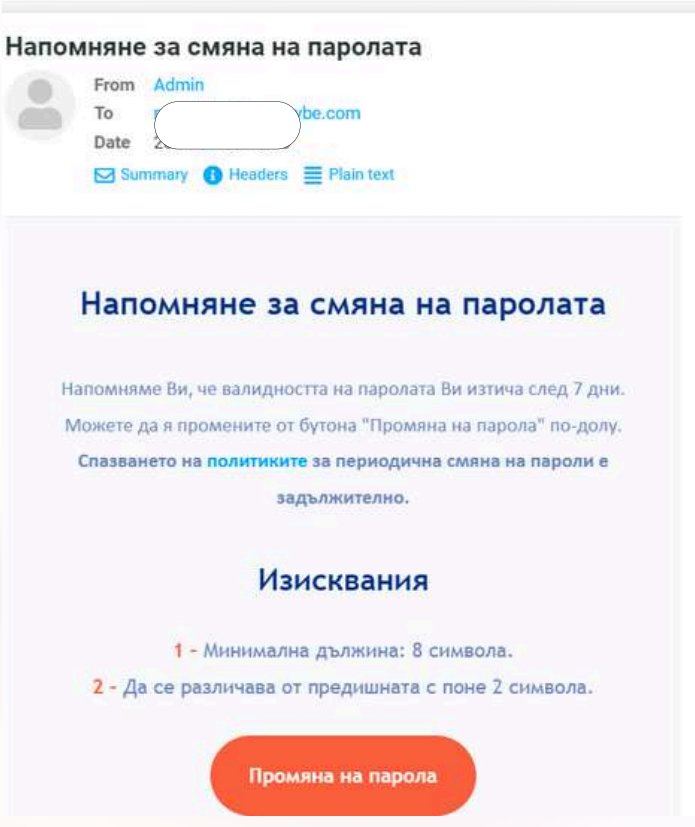
7.3 СИМУЛАЦИИ НА ФИШИНГ АТАКИ И РОЛЕВИ ИГРИ

ЦЕЛ: Повишаване на осведомеността и подготовка на служителите за реални заплахи чрез практическо обучение.

МЕТОДИ:

Въвеждащо обучение:
Основни понятия и принципи на киберсигурността за нови служители.





Ролеви игри:
Инсцениране на инциденти и провеждане на ролеви игри за упражняване на реакциите.

7.4 КАМПАНИИ ЗА ОСВЕДОМЕНОСТ

ЦЕЛ: Повишаване на осведомеността относно кибер заплахите и добрите практики сред служителите.

КОМПОНЕНТИ:

Информационни бюлетини:
Редовни публикации с новини и съвети за киберсигурността.

БЮЛЕТИН ЮНИ 2024 | **БЮЛЕТИН ЮЛИ 2024** | **БЮЛЕТИН АВГУСТ 2024**

Плакати и стикери:
Визуални напомняния в офиса за добри практики по киберсигурност.

ИЗТЕГЛИ АТРАКТИВНИ ПЛАКАТИ ЗА ОФИСА НА ТЕМА “КИБЕРСИГУРНОСТ”

Събития и семинари:
Организиране на събития и семинари за обсъждане на актуални теми по киберсигурност.

ВИДЕОЛЕКЦИЯ КИБЕРСИГУРНОСТ „MODERN IDENTITY SECURITY PLATFORMS“

7.5 ПРОГРАМИ ЗА НЕПРЕКЪСНАТО ОБУЧЕНИЕ

ЦЕЛ: Осигуряване на непрекъснато обучение и развитие на знанията и уменията на служителите.

КОМПОНЕНТИ:

Онлайн курсове:
Достъп до онлайн платформи за обучение по киберсигурност.

ОНЛАЙН ПЛАТФОРМА С КУРСОВЕ ПО КИБЕРСИГУРНОСТ

Сертификационни програми:
Насърчаване на служителите да получават сертификации в областта на киберсигурността.

Менторство и подкрепа:
Създаване на програми за менторство и подкрепа за служителите.

Глава 8

Реакция при Кибер инциденти

Глава 8

8.1 ИДЕНТИФИКАЦИЯ И ДОКЛАДВАНЕ НА ИНЦИДЕНТИ

ЦЕЛ: Осигуряване на бързо и точно идентифициране и докладване на кибер инциденти за минимизиране на щетите.

ОСНОВНИ ЕЛЕМЕНТИ:

Системи за мониторинг:
Използване на инструменти за мониторинг на мрежовия трафик и логове.

Процедури за докладване:
Ясни инструкции за докладване на инциденти от служителите.

8.2 ПРОЦЕДУРИ ЗА ИЗОЛИРАНЕ И ОГРАНИЧАВАНЕ НА ИНЦИДЕНТИ

ЦЕЛ: Ограничаване на разпространението и въздействието на кибер инциденти чрез бързо изолиране на засегнатите системи.

ОСНОВНИ ЕЛЕМЕНТИ:

Изолиране на системи:
Разделяне на засегнатите системи от останалата част на мрежата.

Блокиране на трафик:
Ограничаване на мрежовия трафик към и от засегнатите системи.

Уведомяване:
Уведомяване на всички засегнати страни за предприетите мерки.

8.3 АНАЛИЗ И ВЪЗСТАНОВЯВАНЕ

ЦЕЛ: Анализ на причините за инцидента и възстановяване на нормалната работа на системите.

ОСНОВНИ ЕЛЕМЕНТИ:

Анализ на инциденти:
Определяне на причините и обхвата на инцидента.

Възстановяване на системите:
Възстановяване на засегнатите системи и данни.

8.4 ДОКЛАДВАНЕ И ПРЕВЕНЦИЯ НА БЪДЕЩИ ИНЦИДЕНТИ

ЦЕЛ: Създаване на доклади за инцидентите и предприемане на мерки за предотвратяване на бъдещи инциденти.

ОСНОВНИ ЕЛЕМЕНТИ:

Доклади за инциденти:
Изготвяне на подробни доклади за причините, действията и резултатите от инцидента.

Мерки за превенция:
Анализ на уязвимостите и предприемане на мерки за предотвратяване на бъдещи инциденти.

Глава 9

Примерни политики и ръководства

9.1 ПОЛИТИКА ЗА СИЛНИ ПАРОЛИ

ЦЕЛ: Осигуряване на сигурност на потребителските акаунти чрез използване на силни и уникални пароли.

ОСНОВНИ ЕЛЕМЕНТИ:

Минимална дължина:
Паролите трябва да бъдат най-малко 12 символа.

Сложност:
Паролите трябва да включват главни и малки букви, цифри и специални символи.

Периодична промяна:
Паролите трябва да се сменят на всеки 90 дни.

История на паролите:
Забрана за повторно използване на последните 5 пароли.

Мениджъри на пароли:
Насърчаване използването на мениджъри на пароли за съхранение и управление на паролите.

ИЗТЕГЛИ ПРИМЕРНА ПОЛИТИКА ЗА СИЛНИ ПАРОЛИ

9.2 ПОЛИТИКА ЗА УПРАВЛЕНИЕ НА ДОСТЪПА

ЦЕЛ: Осигуряване на достъп до системи и данни само на оторизирани потребители.

ОСНОВНИ ЕЛЕМЕНТИ:

Идентификация и автентикация:
Всеки потребител трябва да има уникално потребителско име и силна парола.

Ролева база:
Управление на достъпа въз основа на ролите и отговорностите на потребителите (Role-Based Access Control, RBAC).

Двуфакторна автентикация (2FA):
Внедряване на 2FA за всички критични системи.

ИЗТЕГЛИ ПРИМЕРНА ПОЛИТИКА ЗА УПРАВЛЕНИЕ НА ДОСТЪПА.

9.3 ПОЛИТИКА ЗА РЕАКЦИЯ ПРИ ИНЦИДЕНТИ

ЦЕЛ: Осигуряване на бърза и ефективна реакция при кибер инциденти за минимизиране на щетите и възстановяване на нормалната работа.

ОСНОВНИ ЕЛЕМЕНТИ:

Екип за реакция при инциденти (IRT):
Създаване на екип, който е отговорен за управлението на инциденти.

Процедури за докладване:
Ясни инструкции за докладване на инциденти от служителите.

Анализ и възстановяване:
Процедури за анализ на инциденти и възстановяване на засегнатите системи.

ИЗТЕГЛИ ПРИМЕРНА ПОЛИТИКА ЗА РЕАКЦИЯ ПРИ ИНЦИДЕНТИ.

9.4 ПОЛИТИКА ЗА ЗАЩИТА НА ДАННИТЕ

ЦЕЛ: Осигуряване на защита на чувствителните данни от неоторизиран достъп, използване и разкриване.

ОСНОВНИ ЕЛЕМЕНТИ:

Класификация на данните:
Определяне на категории данни въз основа на тяхната чувствителност.

Шифроване:
Използване на шифроване за защита на данните при пренос и съхранение.

Контрол на достъпа:
Ограничаване на достъпа до чувствителни данни до оторизирани потребители.

ИЗТЕГЛИ ПРИМЕРНА ПОЛИТИКА ЗА ЗАЩИТА НА ДАННИТЕ.

Глава 10

Ресурси и инструменти

10.1 ОНЛАЙН КУРСОВЕ И СЕРТИФИКАЦИОННИ ПРОГРАМИ

ЦЕЛ: Осигуряване на възможности за непрекъснато обучение и сертификация в областта на киберсигурността.

ПРЕПОРЪЧАНИ ПЛАТФОРМИ:

Startup Factory:
Видеоуроци и публикации в областта на информационната сигурност, създадени специално за НПО в България.

Всичко за киберсигурността - видео уроци, курсове, блиц съвети и полезни ресурси

Coursera, edX, Udemy:
Онлайн курсове от водещи университети и институции, които покриват основи и напреднали теми по киберсигурност.

CompTIA Security+, CISSP, CEH:
Сертификационни програми, предлагащи задълбочени знания и практическа подготовка.

10.2 ИНСТРУМЕНТИ ЗА МОНИТОРИНГ И ЗАЩИТА

ЦЕЛ: Използване на подходящи инструменти за мониторинг и защита на информационните системи.

ПРЕПОРЪЧАНИ ИНСТРУМЕНТИ:

Антивирусни програми:
Bitdefender, Norton, Kaspersky.

Мениджъри на пароли:
Google Password Manager, LastPass, 1Password, Dashlane.

Системи за откриване и предотвратяване на проникванията (IDS/IPS):
Snort, Suricata.

Мониторинг на мрежовия трафик:
Wireshark, NetFlow.

Резервни копия и възстановяване:
Acronis, Backblaze.

Глава 11

Примери за добри практики

11.1 ИСТОРИИ НА УСПЕХА И ПРОВАЛА

ИСТОРИЯ С УСПЕШЕН КРАЙ:

- **Организация**: НПО за защита на правата на човека
- **Контекст**: Внедряване на политика за силни пароли и двуфакторна автентикация.
- **Резултат**: Намаляване на инцидентите със злоупотреба с акаунти с 80% в рамките на първите шест месеца.
- **Уроци**: Значението на обучението и осведомеността на служителите за новите мерки.

ИСТОРИЯ С НЕГАТИВЕН КРАЙ:

- **Организация**: Малка НПО, предоставяща социални услуги
- **Контекст**: Липса на актуализации на системите и недостатъчно обучение на персонала.
- **Резултат**: Пробив на сигурността, водещ до загуба на чувствителни данни и финансови загуби.
- **Уроци**: Критичната необходимост от редовно актуализиране на софтуера и непрекъснато обучение на служителите.

11.2 АНАЛИЗ НА РЕАЛНИ ИНЦИДЕНТИ

ПРИМЕР 1: ФИШИНГ АТАКА

- **Ситуация**: Служител получава имейл, изглеждащ като от доверен партньор, с искане за актуализация на данни.
- **Действия**: Служителят кликва върху линка и въвежда данни на фалшив сайт.
- **Резултат**: Компрометиране на акаунта и неоторизиран достъп до вътрешни системи.
- **Мерки**: Внедряване на програма за осведоменост за фишинг и настройка на двуфакторна автентикация.

ПРИМЕР 2: РАНСЪМУЕР АТАКА

- **Ситуация**: Зловреден софтуер криптира файлове на сървъра и изисква откуп.
- **Действия**: Липса на резервни копия води до необходимостта от плащане на откупа.
- **Резултат**: Финансови загуби и престой на системите.
- **Мерки**: Внедряване на редовни резервни копия и обучение на персонала за избягване на зловредни линкове.

11.3 ПРЕПОРЪКИ ЗА ВНЕДРЯВАНЕ НА ДОБРИ ПРАКТИКИ

АНАЛИЗ НА РИСКОВЕТЕ:

- Провеждане на редовни оценки на рисковете за идентифициране на потенциалните заплахи и уязвимости.

ПОЛИТИКИ ЗА СИГУРНОСТ:

- Разработване и прилагане на политики за сигурност, включително управление на достъпа, силни пароли и защита на данните.

ТЕХНИЧЕСКИ МЕРКИ:

- Използване на антивирусен софтуер, шифроване на данни и системи за откриване на прониквания (IDS/IPS).

ОБУЧЕНИЕ И ОСВЕДОМЕНОСТ:

- Провеждане на редовни обучения и симулации за осведомяване на служителите относно кибер заплахите и най-добрите практики за сигурност.

МОНИТОРИНГ И ОДИТ:

- Настройка на системи за мониторинг на мрежовия трафик и редовни одити за оценка на ефективността на мерките за сигурност.

Глава 12

Заключение

Глава 12

12.1 ОБОБЩЕНИЕ

Информационната сигурност в НПО: Защита на чувствителните данни и осигуряване на доверие сред бенефициенти и донори е критична задача.

ОСНОВНИ КОМПОНЕНТИ:

- ***Политики и процедури:*** Разработване и прилагане на политики за управление на пароли, достъп, реакция при инциденти и защита на данни.
- ***Технически мерки:*** Внедряване на защитни стени, антивирусен софтуер, шифроване и системи за мониторинг.
- ***Управление на достъпа:*** Осигуряване на идентификация и автентикация, използване на силни пароли и двуфакторна автентикация.
- ***Обучение и осведоменост:*** Редовни обучения и симулации за повишаване на осведомеността на служителите относно кибер заплахите.
- ***Реакция при инциденти:*** Бърза идентификация, изолиране, анализ и възстановяване след инциденти.

12.2 ПЪТНА КАРТА ЗА ПОДОБРЕНИЕ НА КИБЕРСИГУРНОСТТА В НПО

1 ОЦЕНКА НА ТЕКУЩОТО СЪСТОЯНИЕ:

- *Провеждане на детайлна оценка на текущите мерки за сигурност, уязвимости и рискове.*

2 РАЗРАБОТВАНЕ НА СТРАТЕГИИ:

- *Определяне на цели и изисквания за подобрение на информационната сигурност.*
- *Разработване на подробни политики и процедури.*

3 ВНЕДРЯВАНЕ НА МЕРКИ:

- *Внедряване на необходимите технически мерки, като защитни стени, антивирусен софтуер и системи за мониторинг.*
- *Внедряване на програми за обучение и осведоменост на служителите.*

4 НЕПРЕКЪСНАТО ОБУЧЕНИЕ И ОСВЕДОМЕНОСТ:

- *Провеждане на редовни обучения и осведомителни кампании.*
- *Симулации на атаки и ролеви игри за практическа подготовка.*

5 МОНИТОРИНГ И ПРЕГЛЕД:

- *Настройка на системи за мониторинг на мрежовия трафик и анализ на логове.*
- *Редовни прегледи и актуализации на политиките и процедурите за сигурност.*

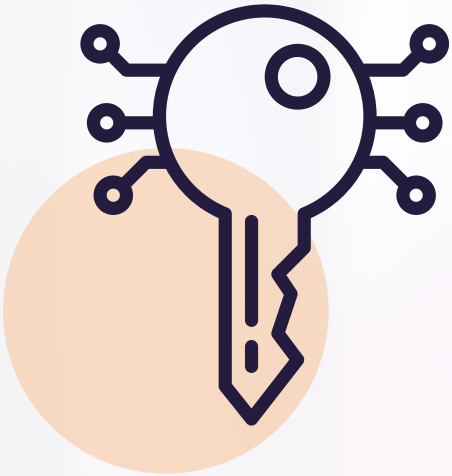
6 АДАПТИРАНЕ КЪМ НОВИ ЗАПЛАХИ:

- *Регулярен преглед на новите заплахи и уязвимости.*
- *Актуализиране на мерките за сигурност и обучение на служителите за новите предизвикателства.*

12.3 РЕСУРСИ, КОНТАКТИ И ПОДКРЕПА

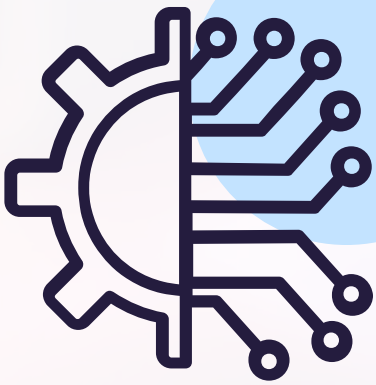
ВЪТРЕШНИ РЕСУРСИ:

- **ИТ отдел:** Основен контакт за всички въпроси и проблеми, свързани с информационната сигурност.
- **Екип за реакция при инциденти:** Отговорен за управлението и разрешаването на кибер инциденти.



ВЪНШНИ РЕСУРСИ:

- **Консултанти по киберсигурност:** Специалисти, които могат да предоставят допълнителна помощ и експертиза.
- **Онлайн курсове и сертификации:** Платформи като Coursera, edX и Startup Factory за непрекъснато обучение.



ОБЩНОСТИ И ФОРУМИ:

- **OWASP:** Ресурси и общности, фокусирани върху сигурността на софтуера.
- **Reddit и Cybersecurity Insiders:** Места за обмен на знания и опит в областта на киберсигурността.

12.4 ЗАКЛЮЧЕНИЕ

Информационната сигурност е непрекъснат процес, който изисква внимание, ангажираност и постоянни усилия. С правилните мерки, обучение и осведоменост, НПО организациите могат да защитят своите данни и да поддържат доверието на своите бенефициенти и донори.

2024

ИНФОРМАЦИОННА СИГУРНОСТ ЗА НПО

© Автор: Теодора Енева, *Startup Factory*

© Редактор: Теодора Енева, *Startup Factory*

© Дизайн: Ана Тодорова, *Startup Factory*

© Издател: *Startup Factory, Русе*

КОНТАКТИ

Сдружение с нестопанска цел “Startup Factory”

Русе, България

startupfactory.bg

0888 796 673

info@startupfactory.bg

Последвайте ни:

STARTUP FACTORY

Финансирано от Европейския съюз

G | M | F Transatlantic Foundation