ОБЩИНА ПОРДИМ , ОБЛАСТ ПЛЕВЕН
5898 гр.Пордим , ул."Иван Божинов"№1 , тел.:06513 / 22 17 , , e-mail: obshtina_pordim@abv.bg

Процедура за управление на инциденти, свързани с информационната сигурност

I. Цел на процедурата

Процедурата за управление на инциденти се определя начинът, по който се реагира при възникване на такъв тип събитие. Описва необходимите действия, които трябва да се предприемат след установяването на възникнал инцидент.

Целта на процедурата е по възможно най-бърз начин да се отреагира при какъвто и да е инцидент и да се намали неговото влияние върху организацията.

II. Роли и отговорности

Настоящата процедура разделя отговорностите и задълженията на служителите на Община Пордим и лица за контакти с оглед осигуряване на информационна сигурност при инцидент, заедно с техните роли и отговорности. Всички трябва да са запознати с тях.

Трябва да се поддържа в актуално състояние списък с контактите на хората, ангажирани в процеса на управление на инцидента като служители и външни фирми, отговарящи за поддръжката и администрацията на системи, приложения и мрежови устройства, както и доставчиците на достъп до Интернет. Този списък се съхранява на достъпни места и на различни носители.

III. Планиране на дейността по управление на инциденти, свързани с информационната сигурност

Дейностите трябва да включват:

- ✓ Определяне списък на възможните инциденти с вероятности за появяването им;
- ✓ Внедрени са технически и организационни механизми за контрол за предпазване възникването на инциденти;
- ✓ Разработен и внедрен процес по инсталиране на актуализации, отстраняващи уязвимости в сигурността на използваните софтуерни продукти, операционни системи и фърмуер на устройствата, особено на тези, които се използват като рутери, защитни стени, сървъри включително и DNS сървъри, мрежови принтери, видеокамери и др. устройства, включени в мрежата на ведомството.
- ✓ Разработен и внедрен процес на резервиране и възстановяване, който да включва:

а) паралелно записване или огледална репликация на съхраняваните данни (технологии "Disk Mirroring" или "RAID-Redundant Array of Independent Drives");

б) създаване на архивно съхранение ("back-up") на информацията от системата, така че да може да се възстанови нейната дейност след инцидента;

- ✓ Процес по установяване и докладване на възникнал инцидент, съгласно закона за киберсигурност;
- ✓ Процес по събиране на информация по определените събития;
- ✓ Процес по установяване и докладване на слабости и уязвимости в сигурността;
- ✓ Процес по определяне на всички засегнати външни и вътрешни ресурси на организацията;
- ✓ Процес по съхранение на събраните доказателства и техния интегритет;
- ✓ Процес по описване на действията извършени в процеса на управление на даден инцидент;
- ✓ Определяне на критично важните функции на системата и установяване на приоритетите за възстановителни работи;
- ✓ Разработка на стратегии за възстановителни работи;
- ✓ Идентификация на ресурсите, необходими за изпълнение на критично важните функции;
- ✓ Процес по намаляване въздействието върху организацията;

IV. Цикъл на управлението на инциденти

Той включва следните основни етапи:

1. подготовка;
2. откриване и анализ;
3. ограничаване на влиянието, премахване на причината, възстановяване;
4. дейности след инцидента.

Всеки един от етапите на управлението на инцидента има своето значение и изисква съответните организационни и технически мерки в зависимост от типа на възникналият инцидент.

В Приложенията са представени разработени процедури за управление на някои най-често случващи се инциденти.

Основни ИТ процедури, които трябва да бъдат изпълнени:

- Създаване на системен имидж – създаване на абсолютен имидж на източниците на информация при инцидент, с цел запазване първоначалната сцена за инцидента;
- Създаване на Screenshots по време на изпълнението на процедурите по управление на инцидента;
- Идентифициране на свидетелите – експерт по разследване на компютърни престъпления, който може да даде свидетелски показания, че всички процедури и политики по управление на даден инцидент са спазени и интегритета на данните е запазен;
- Докладване за инцидент съгласно процедурата на ръководството, на nCERT Bulgaria и на ГДБОП- при наличие на данни за киберпрестъпление;
- Анализ на логовете и корелация на различни събития, за съставяне на цялостната картина по инцидента;
- Възстановяване на работоспособността на системите

- Оценка на щетите и контрол на загубите – след успешното закриване на инцидента се прави оценка на степента на щетите и влиянието им върху организацията.

- Установяване на изработените човеко-часове по даден инцидент, които се включват в общите разходи за управление на инцидента;

- Процес за последващ анализ, ако се изисква такъв;

- Процес по идентифициране на придобития опит;

- Процес по подобряване на механизмите за контрол с цел превенция на бъдещи инциденти;

- Процес по оценка ефективността на предприетите действия по време на инцидента и подобрения;

V. Актуализация на процедурата, ако е необходимо

VI. Утвърждаване на процедурата