

Относно: Мерки за подобряване на информационната сигурност

Във връзка с писмо № 09-00-123/29.07.2019 г. на Министерство на здравеопазването и във връзка с пробивите в сигурността и изтичане на информация от системите на НАП да се пристъпи незабавно към изпълнение на неотложни мерки за подобряване на информационната сигурност, както следва:

1. Да се провери каква организация е създадена за осигуряване на защита на информацията:

\$1 ÿ Какви са прилаганите към момента политики, процедури, вътрешни правила и инструкции;

\$1 ÿ Определени ли са собствениците за всеки информационен актив;

\$1 ÿ Има ли ясно разписани роли и отговорности по отношение на сигурността:

- Кой е отговорният ръководител;
- Кой е системният администратор;
- Кой осъществява контрола над действията;

- Обучени ли са служителите от всички нива;

- Как се реагира при нарушение на сигурността.

2. Да се извърши инвентаризация на всички материални активи, свързани с обработката на информацията:

ü В инвентаризацията да се обхванат компютри, сървъри, принтери, външни памети и т. н.;

ü За всяко устройство да се създаде технически паспорт с подробно описание на всички компоненти, включително хард дискове (в този паспорт да се отбелязват всички промени, подменени или добавени части, ремонти и т. н.).

3. Да се извърши актуализация на системното програмно осигуряване:

ü Операционни системи, офис пакети и т. н.;

ü Да се инсталират всички актуализации (кръпки), препоръчани от производителя и най вече тези, свързани със сигурността;

ü Да се създаде регистър на актуализациите.

4. Да се извърши преглед на използваните други програмни системи:

ÿ Системи за документооборот, заплати, други;

ÿ Каква информация се обработва, къде се съхранява, на кого се предава;

ÿ Кой има достъп до програмите и данните.

5. Да се извърши преглед на използваните системи за сигурност:

ÿ Стандартните възможности на операционните системи;

ÿ Възможностите на защитените стени и конфигурацията им;

ÿ Антивирусни средства.

6. Особено внимание да се обърне върху антивирусната защита:

ÿ Използват ли се антивирусни програми;

ÿ Да се създаде ред за актуализация на антивирусните програми;

ÿ Специално внимание да се обърне за работата с електронната поща (да не се отварят писма от непознати адресати, със съмнително и неясно съдържание и т. н.);

НА ВНИМАНИЕТО НА ВСИЧКИ ЛЕЧЕБНИ И ЗДРАВНИ ЗАВЕДЕНИЯ ОТ ОБЛАСТ МОНТАНА

Написано от РЗИ Монтана
Петък, 30 Август 2019 10:05

\$1ü Да не се посещават електронни страници, които не са свързани с преките задължения;

\$1ü Да се обучат служителите как да реагират при съобщение за вирусна атака.

7. Във връзка с достъпа до информационните ресурси (програми, данни, електронна поща и т. н.):

\$1ü Да се актуализират списъците за достъп (да се изтрият неработещите служители, напуснали такива, тези със сменени функции, външни изпълнители и т. н.);

\$1ü Да се сменят всички пароли за достъп – до компютрите и приложенията (програмите);

Новите пароли да бъдат с минимална дължина 8 символа, големи и малки букви, цифри и символи.

8. Да се направи преглед на системите за физически достъп и да се въведе система за контрол:

\$1ü До районите и сградите;

\$1ü До помещенията с компютри;

\$1ü До помещенията с мрежово оборудване.

9. Да се забрани:

- ü Използване на собствени запаметяващи устройства;

- ü Посещаване на електронни страници, несвързани с изпълнението на задълженията от служителите;

- \$1ü Слушане на музика;

- \$1ü Гледане на филми и видеа;

- \$1ü Инсталирането на неодобри от ръководството софтуери;

- \$1ü Нерегламентирана промяна в конфигурациите на компютрите.

10. Да се актуализират (или да се създадат):

- ü Правила за създаване, използване и достъп до резервни копия на данни;

- ü Правила за сигурно унищожаване на информация за различните видове носители;

- ü Правила за ремонт или подмяна на оборудването.

11. Да се актуализират всички договори от гледна точка на сигурността на информация

НА ВНИМАНИЕТО НА ВСИЧКИ ЛЕЧЕБНИ И ЗДРАВНИ ЗАВЕДЕНИЯ ОТ ОБЛАСТ МОНТАНА

Написано от РЗИ Монтана
Петък, 30 Август 2019 10:05

та:

ÿ За поддръжка на оборудването;

1ÿ За доставка на Интернет услуги;

ÿ Други

При необходимост да се предприемат и други необходими и възможни действия, съгласно предоставената Ви компетентност. За изпълнението на мерките да се изготвят отчетни документи, като протоколи, декларации и др., от които да е видно отговорникът, изпълнителят и времето на изпълнението. Същите да се съхраняват по места.