СПОРТНО УЧИЛИЩЕ "ГЕОРГИ БЕНКОВСКИ" – ВАРНА

Утвърдил:
Евелина Янчева
Директор на СУ „Георги Бенковски“ - Варна

План за действие при киберинциденти, за връщане на системите в предишното им състояние и за техническа профилактика

на СУ „Георги Бенковски" – гр. Варна

Съдържание

1. Управление на инцидентите

2.1. Основни етапи при управление на инцидентите

Включва следните основни етапи:

- Подготовка;
- Откриване и анализ;
- Ограничаване на влиянието, премахване на причината, възстановяване;
- Дейности след инцидента.

Всеки един от етапите на управлението на инцидента има своето значение и изисква служителите от училището да предприемат организационни и технически мерки в зависимост от типа на възникналия инцидент. В документа са представени примерни разработени процедури за управление на някои най-често случващи се инциденти.

2.1.1. Превантивни мерки за намаляване на риска от атаки, ограничаване на последствията и защита от евентуални бъдещи атаки.

1. Актуализиране на схемите на ИТ инфраструктурата и описа на информационните активи на училището

Отговорник:

- Заместник - директор АСД

Срок: веднъж годишно или при изменение.

2. Основен преглед на дейностите и услугите, които училището предлага чрез ИТ инфраструктурата си.

Отговорник:

- Заместник - директор АСД

Срок: два пъти годишно

3. Поддържане в актуално състояние на необходимата информация относно поддръжката и администрирането на ИТ инфраструктурата и системите, списъците с контакти на всички лица и организации, от които зависи поддържането на работоспособността и непрекъсваемостта на дейностите и услугите предоставяни от училището.

Отговорници:

- Заместник - директор АСД

Срок: непрекъснат контрол.

4. Извършване на техническа профилактика на устройствата.

Отговорник:

- Заместник - директор АСД

Срок: непрекъснат контрол, но не по-малко от два пъти годишно.

5. Тестване за уязвимости в мрежовата и информационната сигурност на ИТ инфраструктурата на училището;

Отговорник:

- Заместник - директор АСД

Срок: два пъти годишно

6. Тестване за уязвимости в сигурността на web сайта на училището или други web услуги, които училището предоставя.

Отговорник:

- Заместник - директор АСД

Срок: два пъти годишно.

7. Проверка на достъпите до всички системи и устройства.

Отговорник:

- Заместник - директор АСД

Срок: два пъти годишно, както и при назначаване или преназначаване.

8. Проверка на процеса по резервиране и архивиране на информацията.

Отговорник:

- Заместник - директор АСД
- Софтуерна поддръжка

Срок: минимум два пъти годишно.

9. Организиране на обучения на служителите в училището относно кибер хигиена и добри практики за мрежова и информационна сигурност.

Отговорник:

- Заместник - директор АСД
- ЗАС

Срок: два пъти годишно, както и при назначаване, преназначаване и освобождаване.

10. Ограничаване/недопускане на зловреден софтуер-инциденти и кибератаки.

Отговорник:

- Заместник - директор АСД

Срок: непрекъснат контрол.

2.1.2. Основни ИТ процедури при киберинцидент:

- При възможност да се създаде системен имидж – създаване на абсолютен имидж на източниците на информация по един инцидент, с цел запазване първоначалната сцена за инцидента;
- Създаване на хеш на файлове и бази с цел запазване на техния интегритет и предоставянето им в съда;
- Създаване на Screenshots по време на изпълнението на процедурите по управление на инцидента;
- Докладване за инцидента на РУО – Варна;
- Анализ на логовете и корелация на различни събития, за съставяне на цялостна 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 необходимите човеко-часове по даден инцидент, който се включват към останалите ресурси за управление на инцидента с цел повишаване на ефективността и ефикасността при решаване на подобни инциденти в бъдеще;
- Връзка с плановете за непрекъсваемост на дейността и възстановяване след инцидент;
- Извършване последващ анализ, ако се изисква такъв;
- Процес по идентифициране на придобития опит въз основа на анализа и оказване на насоки за оптимизация от страна на ръководството;
- Процес по подобряване на механизмите за контрол с цел превенция на бъдещи инциденти в зависимост от необходимите ресурсни и организационни мерки;
- Процес по оценка ефективността на предприетите действия по време на инцидента и подобрения;
- Процес по съгласуване и споделяне на научените действия с доверени трети страни и външни доставчици в случай на необходимост.

2.1.2.1. Процедура за реакция при defacement (промяна на изгледа) на уебсайт
Основни причини за Defacement:

- Уязвимости в самите уеб приложения;
- Уязвимости в компоненти, използвани в разработката на уеб сайта (Plugin, AddOn Module и т.н.);
- Неактуализирана операционна система. Уязвимости в услугите на операционната система (Web Server Vulnerability, DB Server Vulnerabolity и т.н.);
- Използване на зададени по подразбиране или слаби пароли за достъп.

Подготовка:

1. Създаване на статично копие на уеб сайта, което да включва основната страница и част от основните секции, които да включват задължително под страници с точките за контакт на гражданите до училището;
2. Създаване на организация по разполагане на архив на уеб сайта (на различна инфраструктура и с достъп до мрежа различна от атакуваната), който при инцидент да заема мястото на основния сайт и стартира процедура за пренасочване на посетителите към него;
3. При възможност с оглед анализ разходи/ползи имплементиране на инструменти за мониторинг с цел бързо засичане на анормално поведение на уеб страницата и предприемане на превантивни мерки за ограничаване на възможно въздействие;
4. Поддържане на актуална схема на мрежовата инфраструктура;
5. Поддържане на актуални контакти на всички, които участват в процеса на поддръжка на системите – на доставчика на Интернет, хостинг доставчика, администратора на приложението, мрежовия администратор.

Идентификация, уведомяване и ограничаване на въздействието:

1. Извършване на мониторинг на уеб страницата, с цел установяване кое съдържание е било променено.

2. Инцидентите се докладват на:
- Началника на РУО – Варна;
- Външен изпълнител, ако страницата се поддържа от такъв;

Ограничаване на въздействието се извършва от длъжностното лице отговорно за поддръжката на сайта и/или от външен изпълнител под контрола на длъжностното лице.

Задължителна стъпка, независимо от обхвата на инцидента е проверка на достъпите и смяна на всички пароли за достъп до сайта.

Възстановяването се извършва от длъжностното лице отговорно за поддръжката на сайта и/или от външен изпълнител съвместно и под контрола на длъжностното лице.

Извличането на поуки/научени уроци от инцидента се.

2.1.2.2. Процедура за реакция при фишинг атака

Съобщение по електронната поща с линк към фишинг сайт

1. Всеки служител уведомява първо длъжностното лице в училище, което от своя страна уведомява директора.
2. Длъжностното лице проверява:

1.Колко и кои потребители на училището са били подложени на фишинг атаката;
2.Проверява URL линка чрез www.virustotal.com или друг сайт за проверка;
3.Определя дали лична или служебна информация е въведена във фишинг сайта;

3. След като се неутрализира атаката се анализира възникналата ситуация:

1.На база резултатите от събраната информация се изготвя доклад относно вида и хронологията на инцидента, предприетите мерки за разрешаването му;
2.Изготвят се препоръки за предприемане на последващи проактивни мерки;
3.Разглеждат се взетите решения и тяхната полза при такъв тим атака;
4.Извършва се анализ на ресурсите, разходвани при решаването на инцидента.

4. При необходимост се актуализират Политиката за мрежова и информационна сигурност, Плана за действие при киберинциденти, за връщане на системите в предишното им състояние и за техническа профилактика на устройствата и анализа на риска.
5. Провежда се кратко обучение на служителите във връзка с конкретния инцидент, като се обръща внимание на пропуските и се дават насоки за превантивни действия в бъдеще на база придобития опит.

Фишинг съобщение по електронната поща с прикачен зловреден файл:

1. Длъжностното лице проверява кои и колко потребители от училището са били подложени на фишинг атаката;
2. Следва се процедурата за реакция при заразяване със злонамерен софтуер описана по-надолу в документа.
3. В случай, че работните станции в училището се управляват от активна директория се създава групова политика (GPO), с която файловете с разширения (.vbs, .vb, .js, .jar, .jsc, .scf, .ws, .wsh, .hta) да се отварят по подразбиране с Notepad до отстраняване на кода.

2.1.2.3. Процедура за реакция при заразяване със злонамерен софтуер

1. При установяване на заразяване със злонамерен софтуер от страна на служителите, незабавно се уведомява длъжностното лице в училище, което от своя страна уведомява директора за възникналата ситуация.
2. Ако са заразени една или няколко системи, за да се предотврати разпространението на зловредния код, незабавно се изключват физически от вътрешната мрежа (чрез отстраняване на кабела за мрежова свързаност или изключване на устройствата за комуникация като Wi-Fi и др.).
3. Ако стъпка 2 не може да бъде извършена своевременно или са заразени значителна част от системите и не са налични защитни стени, изходни филтриращи и прокси сървъри, следва да се блокира ЦЕЛИЯ изходящ трафик, като се премахнат кабелите за достъп до Интернет от централният суич (комутатор).
4. Уведомява се РУО - Варна.
5. С цел изолиране на мрежовите сегменти, в които има заразени системи, в случай на възможност, се конфигурират филтри на вътрешните мрежови устройства. Наблюдава се мрежовия трафик, за идентифициране на потенциални многостранни атаки.
6. Преглеждат се съответните лог файлове, за да се идентифицира първата заразена система и какъв е векторът на атаката, ако е възможно.
7. Проверява се някоя от заразените системи успешно ли се свързва с адрес в Интернет, с който обменя информация.
8. Извършва се анализ, за да се определите обсега на компрометиране и да предприемете подходящи действия за премахване на зловредния код. Не се доверявате на вече инсталирания на системата софтуер, защото той също може да е компрометиран.
9. Ако се установи, че е инсталира rootkit, за всяка заразена система, се прави следното:

1. Установява се наличието на backup на важните данни.
2. Форматира се твърдия диск и се възстановява системата.
3. Установява се, дали всички пачове свързани със сигурността са инсталирани.
4. Променя се името на актива съгласно утвърдената практика за наименование.
5. Инсталира се и се установява, че антивирусната програма е актуализирана до последна версия.
6. Променят се паролите на локалните администратори и на потребителските акаунти за всички системи.

10. При установяване, че системата е заразена с malware се изпълняват следните дейности:

1. Установяване дали всички пачове свързани със сигурността, са инсталирани.
2. Сканират се заразените машини, използвайки антивирусна система с дефиниции, за които е сигурно, че засичат съответния malware.
3. Променят се паролите на локалните администратори и на потребителските акаунти на всички системи.

11. След като всички системи са изчистени, внимателно се следи за повторно заразяване.
12. След като се премахне зловредния софтуер, се анализира ситуацията.

1. На база резултатите от събраната информация се изготвя доклад относно вида и хронологията на инцидента, предприетите мерки за разрешаването му.

2.Изготвят се препоръки за предприемане на последващи проактивни мерки.
3.Разглеждат се взетите решения и тяхната полза при премахването на зловредния софтуер.
4.Извършва се анализ – какви ресурси са изразходвани при тази ситуация с цел повишаване ефективността и ефикасността при решаването им в бъдеще.
5.Провежда се кратко обучение на служителите във връзка с конкретния инцидент, като се обръща внимание на пропуските и се дават насоки за превантивни действия в бъдеще на база придобития опит.

13. При необходимост се актуализират Правила за мрежова и информационна сигурност, План за действие при киберинциденти, за връщане на системите в предишното им състояние и за техническа профилактика на устройствата и Риск анализа.

2.1.2.4. Действия от служителите в случаи на заразяване с компютърни вируси и кибератаки от тип Ransomware (процес при който се криптират част или всички файлове на заразената машина и се визуализира съобщение за откуп):

1. Да се изключат заразените машини от мрежата (чрез отстраняване на кабела за мрежова свързаност или изключване на устройствата за комуникация като Wi-Fi и др.) и да се направят резервни копия на данните, за да се избегне вероятността тези данни също да бъдат криптирани, в случай на оставане в мрежата.
2. Предприемат се следните стъпки:

- При всяко съмнение за кибератака и заразяване със зловреден софтуер от този тип, незабавно се уведомява длъжностното лице
- Спира се възможно най-бързо достъпа на заразения компютър до мрежата (вътрешна и външна).
- Не се изключва захранването на заразените компютри и те не се рестартират.
- Не се плаща искания откуп.
- В много от случаите декриптирането на файловете е невъзможно.
- Установява се, в какво разширение файловете биват криптирани. На сайта https://www.nomoreransom.org се намира професионална помощ за най-различни семейства от ransomware.
- Създаване на резервно копие на празен външен носител на най-важните данни, ако ситуацията позволява.
- Преди включване на компютрите отново, предварително трябва да сме сигурни, че е изцяло поправена и актуализирана операционната система.
- Уведомява се РУО - Варна.
- При необходимост се актуализират Правила за мрежова и информационна сигурност, План за действие при киберинциденти, за връщане на системите в предишното им състояние и за техническа профилактика на устройствата и Риск анализа.
- Провежда се кратко обучение на служителите във връзка с конкретния инцидент, като се обръща внимание на пропуските и се дават насоки за превантивни действия в бъдеще на база придобития опит.

2.1.2.5. Действия в случаи на атака към мрежовата инфраструктура на училището:

1. В случай на смущения в работата на информационните системи се предприемат следните стъпки:

- Определя се дали смущенията се дължат на DDoS атака или има друга причина (проблем с неправилно конфигуриране на DNS, проблеми с рутирането или човешка грешка).
- Проверка на изходящи връзки. Ако няма изходящи връзки, то атаката е толкова силна, че задръства целия входящ и изходящ трафик. Проверката се извършва с обичайните инструменти за диагностика (като traceroute, ping и dig).
- Проверка на достъпа по IP адрес и по url до онлайн услуги от външни мрежи.
- Проверка на логовете на различни мрежови устройства и сървъри, участващи в предоставянето на засегнатата услуга. Логовете трябва да се съхранят на отделна машина.
- След установяване на атака длъжностното лице уведомява:
  - Директор;
  - Доставчиците на Интернет услуги - те може да потвърдят атаката, да предоставят информация кои други клиенти, биха могли да бъдат засегнати от атаката, да предложат механизми за смекчаване.
- Вземане на решение кои услуги да бъдат спрени - услуги с нисък приоритет, трябва да бъдат целенасочено изключени, за да може процесорите и паметта на устройствата и мрежовите ресурси да обслужват услугите и приложенията с по-висока важност и значимост.
- Оценяване на възможностите за смекчаване на атаката чрез въздействие на IP адресите на източниците на трафика. Според броя на източниците на атака, в случай на възможност, се използва блокиране от защитната стена или геоблокиране.
- Провежда се кратко обучение на служителите във връзка с конкретния инцидент, като се обръща внимание на пропуските и се дават насоки за превантивни действия в бъдеще на база придобития опит.

Всички служители на училището имат задълженията да съблюдават плана при възникване на инцидент.