ОБЩИНА МОНТАНА

3400 МОНТАНА, ул."Извора"1, тел:(096) 300 400, факс: (096) 588 391,E-mail: mayor@montana.bg

Утвърждавам:

Златко ЖИВКОВ

КМЕТ на община МОНТАНА

ПРОЦЕДУРА ПРИ УПРАВЛЕНИЕ НА ИНЦИДЕНТИ, СВЪРЗАНИ С ИНФОРМАЦИОННАТА СИГУРНОСТ

Цел на процедурата

Процедурата за управление на инциденти в Община Монтана определя начина, по който се реагира при възникване на такъв тип събитие. Подробно описва необходимите действия, които трябва да се предприемат, след установяването на възникнал инцидент.

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

Роли и отговорности

Роли и отговорности свързани с управление на инциденти в Община Монтана:

1. Системен администратор

Роля: Отговорен е за управлението и защитата на информацията. Предприема всички необходими мерки касаещи информацията, и контрола за интегритет и конфиденциалност.

Отговорности:

- Разбира основните рискове от цялостната употреба на специфична информация;

- Определя нивото на чувствителност на информацията;

- Дефинира допълнителни методи за защита;

- Одобрява искания на потребители за достъп;

- Преглежда списъка за достъп на потребителите и определя или отнема права.

2. Потребители – служители на отдели и дирекции.

Роля: Служителите на общинската администрация, които имат достъп до данните на информационните системи.

Изискват от системния администратор права за достъп;

- Не използват информационни активи без лична идентификация;
- Докладват за грешки и инциденти на системния администратор и служителя по сигурността.

3. Списък с контактите на специалистите, ангажирани в процеса на управление на инциденти:

Служители на Община Монтана:

Бисера Димитрова – началник отдел ЦУИГ

телефон: 096 394 220 ; електронна поща: cuig@montana.bg

Николай Драгиев – старши експерт „Информационни технологии“

телефон: 096 394 226 ; електронна поща: ndragiev@montana.bg

Крум Крумов – служител по сигурността на информацията

телефон: 096 394 264; електронна поща: omp@montana.bg

Външни фирми, отговарящи за поддръжката и администрацията на информационните системи

„Електрон М“

Представител : Веселин Дяков

телефон: 0887 772471 ; електронна поща: kezisoft@yahoo.com

Планиране на дейността по управление на инциденти, свързани с информационната сигурност включва:

- Политиката за информационна сигурност и Стратегия за управление на риска в Община Монтана утвърдена със заповед на кмета на Община Монтана;
- Списък на възможните инциденти с вероятности за появяването им, изхождайки от оценките на риска;
- Утвърдени Вътрешни правила за мрежова и информационна сигурност;
- 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:

- автоматизирано и планово се извършва архивиране на цялата работна информация на сървърите и дисковите масиви.

- архивирането на данните се извършва по начин, който позволява, при необходимост данните да бъдат инсталирани на друг сървър. Допълнително се архивират целите виртуални машини за да може при необходимост да се възстанови компрометирания сървър и продължи работният процес без чувствителна загуба на данни;

б) Създаден център за възстановяване след инциденти (т.нар. "Disaster Recovery Center"), в който се извършва постоянно архивно съхранение (Backup) на информацията от системата, така че да може да се възстанови нейната дейност след инцидента;

4. Цикълът на управление на възникнали инциденти в включва следните основни етапи:

а) подготовка;

б) откриване и анализ;

в) ограничаване на влиянието, отстраняване на причината, възстановяване;

г) 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.

5. В приложенията са представени примери на разработени процедури за управление на някои най-често случващи се инциденти в, а именно:

Приложение 1 - Процедура за реакция при присвояване на уебсайт;

Приложение 2 - Процедура за реакция при DDoS атака;

Приложение 3 - Процедура за реакция при заразяване със злонамерен софтуер;

Приложение 4 - Процедура за реакция при фишинг атака.

Основни ИТ процедури, които трябва да бъдат изпълнени при управлението на възникнал инцидент:

- Създаване на 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;

- 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;

- 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;

- Връзка с плановете за непрекъсваемост на дейността и възстановяване след инцидент;

- 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;

- Процес по съгласуване и споделяне на научените действия с доверени трети страни;

Процедура за реакция при присвояване на уебсайт www.iag.bg:

Подготовка

1. Необходимо е да разполагаме с актуални схеми, които описват компонентите на уеб сървъра.
2. Необходимо е да разполагаме с архив на уеб сайта, който при инцидент да заеме мястото на основния сайт и да се стартира процедурата за пренасочване на посетителите към него.
3. Имплементиране на инструменти за мониторинг с цел бързо засичане на анормално поведение на уебсайт www.montana.bg.
4. Възможност за експортиране на лог файловете на уеб сървъра във външен сървър (Log Management Server/ SIEM).
5. Поддържане на актуална схема на мрежовата инфраструктура.
6. Поддържане на актуални контактите на участващите в процеса по поддръжка на системите - доставчика на достъп до интернет, администратора на приложението, мрежовия администратор, nCERT България, ДАНС и ГДБОП.

Идентификация

1. Извършване мониторинг на уеб страницата с цел установяване кое съдържание е било променено.
2. Извършване проверка на сигурността на уеб сайта с инструменти като Google SafeBrowsing.
3. Процедура по установяване на defacement и определене на неговия произход:
   - Проверка на датите на модифициране на файловете и техните хешове.
   - Проверка mashup content providers.
   - Проверка на линковете в уеб страницата (src, meta, css, script, …).
   - Проверка на лог файловете.
   - Сканиране на базите данни за зловредно съдържание.
4. Докладване за инцидента на
   - Ръководството
   - nCERT Bulgaria (до 2 часа съгласно закона за КС)
   - ДАНС, ако е обект със стратегическо значение
   - ГДБОП, ако има данни за киберпрестъпление

Ограничаване на въздействието

1. Изключване на компрометираният сървър от мрежата
2. Направа на архив на всички данни на уеб сървъра с цел forensic анализ и събиране на доказателства. Най-добрата практика, ако е приложима, е bit-by-bit копие на хард диска на уеб сървъра. Това би помогнало и за възстановяване на изтрити файлове.

3. Проверка схемата на мрежовата инфраструктура. Уверяваме се, че уязвимостта, която е използвана, не се намира другаде.
   - Проверка на системата, на която уеб сървърът работи.
   - Проверка какви други услуги работят на същата машина.
   - Проверка на връзките с други системи и дали някоя от тях е компрометирана.
4. Ако източникът на атаката е друга система от мрежата, се осигурява изключването и от мрежата, по възможност и се предприемат действия по изследването и.
   - Установяване на това, коя техника е използвал атакуващия, коя е първоначално пробитата система ;
   - Уязвимост на уеб компоненти: поправяне на уязвимостта, използвайки съответния пач.
   - Open public folder: fix the bug
   - Уязвимост към SQL инжекции: коригирайте кода.
   - Mashup components: cut mashup feed.
   - Модификация с административни права чрез физически достъп: променяне правата за достъп.
5. Ако е необходимо при сложен проблем и много важен уеб сървър, вдигане на временен уеб сървър, актуален с неговите приложения. Той трябва да предлага същото съдържание, като компрометирания уеб сървър или най-малкото да показва друго легитимно съдържание, като „Сайтът е временно недостъпен ". Най-добре е да се покаже временно статично съдържание, съдържащо само HTML код. Това предотвратява друга инфекция в случай че атакуващият е използвал уязвимостта в PHP / ASP / CGI / PL /и т.н. код.

Възстановяване

1. Премахваме съдържанието, което е подменено и възстановяваме оригиналното.
2. Поправяме на намерените уязвимости.
3. Възстановяваме съдържанието, използвайки последния архив и се уверяваме, че съдържанието не съдържа уязвимости (ако уязвимите източници са от самите уеб приложения).
4. Преглед на операционната система на уеб сървъра за подозрителни процеси и/или наличие на Backdoor/Rootkit и отстраняването им, използвайки някой от предложените инструменти:
   - Chkrootkit: http://www.chkrootkit.org/
   - Rkhunter: http://rkhunter.sourceforge.net/
   - Linux Malware Detect: https://github.com/rfxn/linux-malware-detect
   - MalDet: https://github.com/dkhuuthe/MalDet
   - ClamAV: https://www.clamav.net/
   - MalScan: https://github.com/mtingers/malscan
   - NeoPi: https://github.com/Neohapsis/NeoPI

5. Проверка за качен PHP Backdoor / Web Shell / Backdoor Shell чрез някой от предложените инструменти:

- http://www.shelldetector.com/
- http://www.whitefirdesign.com/tools/basic-backdoor-scriptfinder.html
- http://resources.infosecinstitute.com/web-shell-detection/
- http://25yearsofprogramming.com/blog/2010/20100315.htm
- http://resources.infosecinstitute.com/checking-out-backdoorshells/
- https://bechtsoudis.com/hacking/detect-protect-from-phpbackdoor-shells/

6. Промяна на всички потребителски пароли, ако уеб сървърът изисква потребителска автентикация и/или ако имаме съмнения или доказателства за компрометирани акаунти.

7. Ако временно сме използвали архив на уеб сървъра (т.2 от Подготовка) , въвеждаме основния обратно в експлоатация.

8. Документираме подробно всяка стъпка от процеса на управление на инцидента

9. Използваме комуникационната стратегия ако defeicment страницата е била видима за част от потребителите и планираме публичното оповестяване на инцидента.

10. Изготвяне на подробен доклад за инцидента и осигуряване на достъпност за всички участващи страни. Трябва да се съдържа минимум:

- Първоначално откриване;
- Действия и срокове;
- Какво се случи;
- Какво се обърка;
- Разходи за инциденти.

11. Изпращаме подробен доклад на nCERT България до 5 дни след установяване на инцидента.

Извлечени поуки / научени уроци от инцидента

- В случай на откриване на уязвимост, докладваме на всички за недокументираната уязвимост, лежаща върху работещ продукт на уеб сървъра (като PHP форум) на неговия редактор, така че кодът може да бъде надстроен, за да се разработи поправка.

- Укрепване на инфраструктурата (Web Server, DB Server)

- Актуализация на уеб приложението (преглед на изходния код, Penetration Testing)

- Имплементираме Web Application Firewall (в случай че няма)

- Имплементираме IDS / IPS (в случай че няма) или настройка на правилата

- Имплементираме File Integrity Monitoring

- Имплементираме програма за управление на обновяванията

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 Vuln, DB Server Vuln и т.н.)

Приложение 2

Процедура за реакция при фишинг атака:

Е-мейл с линк към фишинг сайт

1. Проверка на това колко потребители в организацията са били подложени на фишинг атаката.
2. Определяне на това дали лична или корпоративна информация е въведена във фишинг сайта.
3. Уведомяване на ръководството за възникналата ситуация, в зависимост от вътрешните правила.
4. Докладване за настъпилия инцидент на CERT България до 2 часа след неговото установяване.
5. След като се неутрализира атаката, анализиране на възникналата ситуация:

✓ На база резултатите от събраната информация изготвяне на доклад относно вида и хронология на инцидента, предприетите мерки за разрешаването му.

✓ Изготвяме препоръки за предприемане на последващи проактивни мерки.

✓ Разглеждаме взетите решения и тяхната полза при фишинг атаката.

✓ Извършваме анализ, какви ресурси са изразходвани при тази ситуация.

✓ Помисляме и над факта какви ресурси, било то външни или вътрешни, биха могли да помогнат при бъдещи подобни ситуации.

6. При необходимост обновяване на процедурата.
7. Изпращаме подробен доклад на CERT България за причините, довели до фишинг атаката и предприетите действия.

Фишинг е-мейл с прикачен зловреден файл:

1. Проверка на това колко потребители в организацията са получили въпросния е-мейл.
2. Следваме **Процедура за реакция при заразяване със злонамерен софтуер**.
3. Създаваме групова политика (GPO) в Активната Директория забрана за активиране и изпълнение на макроси в Microsoft Office.
4. Създаваме групова политика (GPO) в Активната Директория, с която файлове с разширения (.vbs, .vb, .js, .jar, .jsc, .scf, .ws, .wsc, .wsh, .hta) да се отварят по подразбиране с Notepad.
5. Повтаряне на стъпки след точка 5 от предната процедура.

Приложение 3

Процедура за реакция при DDoS атака

1. Определяме точките на отказ от услуги.
    a. DDoS нападателите се насочват към всяка потенциална точка на отказ като web сайтове, web приложения, приложни програмни интерфейси (APIs), domain name system (DNS), сървъри, центрове за данни и мрежова инфраструктура.
2. Уведомяваме ръководството за възникналата ситуация, в зависимост от вътрешните правила във вашата организация
3. Докладваме за настъпилия инцидент на CERT България до 2 часа след неговото установяване.
4. Свързване с доставчика на интернет услуги за да уточним мащаба на DDoS атаката и нейното смекчаване.
5. Проверяваме всички устройства, сървъри и приложения да са актуализирани до последна версия.
6. Ако не сте администратор на атакуваната система или устройства е необходимо да се свържете със съответния администратор.
7. Свързваме се с фирмата, поддържаща Вашите устройства, ако има такава.
8. Архивираме логовете от всички засегнати устройства (сървъри, рутери, защитни стени и др.) и ги анализираме, използвайки приложения за анализ на мрежовия трафик.
9. Създаваме ACL за приоритизация на трафика.
10. Осигуряваме алтернативна комуникационна свързаност чрез VPN за критичните за Вас услуги.
11. Използваме Reverse path forwarding (RPF).
12. Филтрираме входящия и изходящия трафик.
13. Задаваме лимити на:

- скоростта на преминаващите ICMP пакет,
- скоростта на преминаващите SYN пакет,
- DNS TTL за атакуваните системи,

14. Търсене модели на трафика, за да идентифицирате познати атаки.
15. Разбираме дали сме обект на атаката или косвена жертва.

16. Идентифицираме атакуващите IP адреси и ги проследете в лог файловете, за злонамерени действия преди началото на атаката.
17. Сканиране на устройствата за зловреден софтуер, влязъл при атаката.
18. По възможност изключваме всички неизползвани по време на атаката устройства.
19. Идентифицираме и локализираме DDoS трафика от реалния трафик.
20. При възможност използваме геофилтриране.
21. Извършваме контрол на content delivery на база на потребител и сесия.
22. Ако е възможно, преминаваме към алтернативна мрежа.
23. Ако атаката е към конкретно приложение, обмисляме варианта временно да го спрем.
24. При възможност добавяме допълнителни ресурси, като сървъри или мрежови устройства. Целта ще бъде да запазим услугата онлайн докато отстраняваме проблема.
25. Извършваме промените постепенно. При промяна изчакаме малко, за да разгледаме ефекта от нея и при необходимост след това, въведем други промени.
26. Въвеждаме филтри относно отговора на сървърите към DDoS трафика. Така ще филтрираме допълнително изпращане на пакети по мрежата ви.
27. След като неутрализираме атаката, трябва да анализираме възникналата ситуация:
28. Преценяваме какви предварителни действия можете още да предприемете.
29. Разглеждаме взетите решения и тяхната полза при атаката.
30. Извършшаме анализ какви ресурси са изразходвани при тази ситуация.
31. Помисляме и над факта какви ресурси, било то външни или вътрешни, биха могли да ви помогнат при бъдещи подобни ситуации.
32. При необходимост обновяваме процедурата.
33. Изпращаме подробен доклад на CERT България за причините до довели до атаката и предприетите действия.

Приложение 4

Процедура за реакция при заразяване със злонамерен софтуер

1. Ако са заразени една или няколко системи, незабавно ги изключваме физически от вътрешната мрежа, за да предотвратим разпространението на зловредния код и свързването им със C&C сървъра.

2. Ако стъпка 1 не може да бъде извършена своевременно или са заразени значителна част от системите и не сме въвели силни защитни стени, изходни филтриращи и прокси сървъри, незабавно трябва да блокираме ЦЕЛИЯ изходящ трафик към външни мрежи.

3. Уведомяваме ръководството за възникналата ситуация, в зависимост от вътрешните правила в .

4. Докладване за настъпилия инцидент на CERT България до 2 часа след неговото установяване.

5. Конфигуриране филтри на вътрешните мрежови устройства с цел изолиране на мрежови сегменти, в които има заразени системи. Наблюдаване мрежовия трафик, за идентифициране на потенциални многостранни атаки.

6. Преглеждаме подходящите лог файлове, за да се опитаме да идентифицираме първата заразена система и какъв е векторът на атаката, ако е възможно.

7. От важно значение е да определим дали някоя от заразените системи успешно се свързва със сайт в Интернет, с който обменя информация.

8. Извършваме forensic анализ на системата, идентифицираме в стъпка 6, за да определяме обсега на компрометиране и да предприемем подходящите действия за премахване на зловредния код. Не се доверяваме на вече инсталирания на системата софтуер, защото и той също може да е компрометиран.

9. Ако установим, че е инсталиран rootkit, за всяка заразена система, правим следното:

- Да се уверим, че имате backup на важните данни.
- Да форматираме твърдия диск и да възстановим системата.
- Да се уверим, че всички пачове, свързани със сигурността, са инсталирани.
- Да се уверим, че антивирусната ви програма е актуализирана до последна версия.
- Да променим паролите на локалните администратори и на потребителските акаунти за всички заразени системи.

10. Ако установим, че системата е заразена с малуер, правим следното:
    - Да се уверим, че всички пачове, свързани със сигурността, са инсталирани.
    - Да сканираме заразените машини, използвайки антивирусна система с дефиниции, за които е сигурно, че засичат съответния малуер.
    - Да променим паролите на локалните администратори и на потребителските акаунти за всички заразени системи.

11. След като всички системи са изчистени, внимателно следим за повторно заразяване.

12. След като премахнем зловредния софтуер, анализираме ситуацията:

✓ На база резултатите от събраната информация изготвяме доклад относно вида и хронология на инцидента, предприетите мерки за разрешаването му.
✓ Изготвяме препоръки за предприемане на последващи проактивни мерки.
✓ Разгледаме взетите решения и тяхната полза при премахването на зловредния софтуер.
✓ Извършване на анализ какви ресурси са изразходвани при тази ситуация.
✓ Анализ какви ресурси, било то външни или вътрешни, биха могли да ви помогнат при бъдещи подобни ситуации.

13. При необходимост обновяване на процедурата.
14. Изпращане на подробен доклад на CERT България за създалата се ситуация и предприетите действия.