



МИНИСТЕРСТВО НА ОБРАЗОВАНИЕТО И НАУКАТА

ЦЕНТЪР ЗА СПЕЦИАЛНА ОБРАЗОВАТЕЛНА ПОДКРЕПА „Св. Св. Кирил и Методий“

с.Кривня, общ.Провадия, обл.Варна, тел./факс: 0518/4 1312, 0878273413,

e-mail: info-4001612@edu.mon.bg; csop_metodii@abv.bg

Утвърдил – Директор



ВЪТРЕШНИ ПРАВИЛА

ЗА МРЕЖОВАТА И ИНФОРМАЦИОННАТА

СИГУРНОСТ

В ЦСОП „СВ.СВ КИРИЛ И МЕТОДИЙ“.С.КРИВНЯ

За учебната 2025/2026 година

В сила от 15.09.2025год с решение на ПС Протокол № 07/ 09.09.2025 г

РАЗДЕЛ I

ОБЩИ ПОЛОЖЕНИЯ

Чл. 1 Настоящите правила имат за цел осигуряването на контрол и управление на работата на информационните системи в ЦСОП "Св.св Кирил и Методий" с.Кривня. В този смисъл понятието информационна система се определя като съвкупност от компютърна и периферна техника, програмни продукти, данни и обслужващ персонал, като компютрите могат да бъдат свързани в локална мрежа или по друг начин, както и да обменят информация чрез съответните устройства и програми. Програмните продукти и бази данни могат да бъдат специфични за всяко звено от администрацията или с общо предназначение.

Чл. 2 (1) Потребителите на информационни системи в ЦСОП "Св.св Кирил и Методий" с.Кривня. са задължени с отговорни действия да гарантират ефективното използване на системите.

(2) ИКТ специалиста предлага и реализира концепция за защита и опазване на електронните бази данни.

Чл. 3 Създаването, разместването, преконфигурирането на работни места в центъра, на чието разположение са или се предвижда да бъдат предоставени компютърни конфигурации се съгласува с ИКТ специалиста(Радостин Боев- възпитател).

Чл. 4 (1) Проектирането и изграждането на информационни и комуникационни системи се извършва така, че те да представляват компоненти с възможност за интеграция в единна потребителска среда и при спазване на Българската национална рамка за оперативна съвместимост на информационните системи в изпълнителната власт, Наредбата за общите изисквания за мрежова и информационна сигурност и Наредбата за общите изисквания към информационните системи, регистрите и електронните административни услуги.

(2) Техническото осигуряване с компютърна и периферна техника се избира с оглед на изискванията на програмните продукти, които ще се използват на съответното работно място, както и със състоянието и тенденциите за развитие на компютърните технологии.

РАЗДЕЛ II

КОНТРОЛ НА ДОСТЪПА И ПРАВИЛА ЗА РАБОТА С НОСИТЕЛИ

Чл.5 Защитата и контролът на информационните и компютърните системи се извършва при спазване на следните основни принципи:

1. разделяне на потребителски от администраторски функции;
2. установяване на нива и достъп до информация;
3. регистриране на достъпа, въвеждането, промяната и заличаването на данни и информация;

Чл. 6 Всеки служител има точно определени права на достъп и използва уникален потребителски профил за вход в системата и достъп до данните, за които е оторизиран, така че да може да бъде идентифициран.

Чл. 7 Контрол на управлението и защитата на достъпа до мрежови връзки и мрежови услуги се извършва чрез средствата на активна директория с конкретно потребителско име, осигурено от специалист ИКТ, който контролира компютрите, използвани за достъп до мрежи и мрежови услуги.

Чл. 8 (1) Ръководството на ЦСОП“Св.св Кирил и Методий“ с.Кривня. задава определени права на достъп до конкретни информационни ресурси, според заемната длъжност, съгласно разписани функции в длъжностната характеристика или заповед за оправомощаване. Не се задава и не се осигурява достъп на неоторизирани лица.

(2) При прекратяване на служебно или трудово правоотношение се прекратяват правата на достъп до мрежови ресурси, електронната поща и при необходимост за преинсталиране на персоналния компютър на освободения от длъжност служител.

Чл. 9 Служителите, които обработват лични данни, използват уникални пароли с достатъчно сложност, които не се записват или съхраняват онлайн.

Чл. 10 Всички пароли за достъп на системно ниво се променят периодично.

Чл. 11 Във Вътрешните правила за мерките за защита на личните данни в ЦСОП“Св.св Кирил и Методий“ с.Кривня. се регламентират мерки за защитата на автоматизираните информационни системи и мрежи.

Чл. 12 На служителите на ЦСОП“Св.св Кирил и Методий“ с.Кривня., които използват електронни бази данни и техни производни (текстове и разпечатки) се забранява:

1. да ги изнасят под каквато и да е форма извън служебните помещения;
2. да ги използват извън рамките на служебните си задължения;
3. да ги предоставят на външни лица.

Чл. 13 За нарушение целостта на данните се считат следните действия:

1. унищожаване на бази данни или части от тях;
2. повреждане на бази данни или части от тях;
3. вписване на невярна информация в бази данни или части от тях.

Чл. 14 При изнасяне на носители извън физическите граници на ЦСОП“Св.св Кирил и Методий“ с.Кривня. те се поставят в подходяща опаковка и в запечатан плик.

Чл. 15 На служителите е строго забранено да използват мобилни компютърни средства на места, където може да възникне риск за средството и информацията в него. Потребителите на мобилни компютърни средства и мобилни телефони отговарят за защитата им от кражба и не ги оставят без наблюдение.

Чл. 16 Служителите са длъжни да избягват всякакъв риск от достъп до информация от неупълномощени лица, както и до злоумишлен софтуер. Забранено е съобщаването на

служебна информация по мобилни телефони на места, където може да стане достъпна за трети страни.

Чл. 17 След като повече не са необходими, носителите се унищожават сигурно и безопасно за намаляване на риска от изтичане на служебна информация към неупълномощени лица. Физическото унищожаване на информационните носители става със счупване. Предварително се проверят, за да е сигурно, че необходимата информация е копирана и след това цялата информация е изтрита от тях преди унищожаване.

Чл.18 Публикуването на данни и информация на официалната интернет страница на ЦСОП“Св.св Кирил и Методий“ с.Кривня. се извършва от определен за това служител – Радостин Боев изпълняваща длъжността възпитател .

Чл.19 Събирането и подготовката на данните се извършва от служители в техния ресор, след което данните се изпращат в електронен вид (на файлове) на служителя по чл. 17 от тези правила.

РАЗДЕЛ III

РАБОТНО МЯСТО

Чл. 20 Работното място се състои от работно помещение, работна маса и стол, компютърна и периферна техника, комуникационни средства.

Чл. 21 Работното място се оборудва при спазване на изискванията на Наредба № 7 от 15.08.2005г. за минималните изисквания за осигуряване на здравословни и безопасни условия на труд при работа с видеодисплеи.

Чл.22 Сървъри на локални компютърни мрежи се разполагат в самостоятелни помещения съобразно изискванията на Приложение № 11 към чл. 45, ал. 2 от Наредба за общите изисквания за мрежова и информационна сигурност.

Чл.23 Всеки служител отговаря за целостта на компютърната и периферна техника, програмните продукти и данни, инсталирани на компютъра на неговото работно място или ползвани от него на сървъра на локалната компютърна мрежа съобразно дадените му права. Чл.24 Служителят има право да работи на служебен компютър, като достъпът до съхраняваните данни се осъществява от него с въвеждането на потребителско име и парола.

Чл.25 (1) Забранява се на външни лица работата с персоналните компютри на ЦСОП“Св.св Кирил и Методий“ с.Кривня., освен за отговорния за това служител при спазване на строга поверителност.

(2) Инсталирането и актуализацията на програмни продукти се извършва единствено от ръководител на направление ИКТ.

Чл.26 След края на работния ден всеки служител задължително изключва компютъра, на който работи, или го привежда в режим log off.

Чл.27 При загуба на данни или информация от служебния компютър, служителят незабавно уведомява ръководител на направление ИКТ.

Чл.28 Забраняват се опити за достъп до компютърна информация и бази данни, до които не са предоставени права, съобразно заемащата от служителя длъжност, както и извършването на каквито и да е действия, които улесняват трети лица за нерегламентиран достъп.

Чл.29 Инсталиране и размястване на компютърни конфигурации и части от тях, на периферна техника, на активни и пасивни компоненти на локални компютърни мрежи, на комуникационни устройства се извършва само от ръководител на направление ИКТ.

Чл.30 Служителите имат право да обменят компютърна информация посредством вътрешна компютърна мрежа само във връзка с изпълнение на служебните си задължения и само със служителите, с които имат преки служебни взаимоотношения.

Чл.31 Архивирана компютърна информация се предоставя само на служители, които имат право на достъп, съгласно заемащата от тях длъжност и изпълнявана задача, при спазване на принципа „необходимост да се знае.“

Чл.32 Достъпът до компютърна информация, бази данни и софтуер се ограничава посредством технически методи - идентификация на потребител, пароли, отчитане на времето на достъп, забрани за копиране, проследяване на нерегламентиран достъп.

Чл.33 Достъпът до помещенията, където са разположени сървърите и комуникационните шкафове се ограничава само до специализиран по поддръжката им персонал.

РАЗДЕЛ IV

ПОЛЗВАНЕ НА КОМПЮТЪРНАТА МРЕЖА И ИНТЕРНЕТ

Чл.34 Ръководителят на направление ИКТ извършва необходимите настройки за достъп до интернет, създават потребителски имена и пароли за работа с компютърната мрежа и електронната поща на ЦСОП“Св.св Кирил и Методий“ с.Кривня..

Чл.35 Ползването на компютърната мрежа и електронната поща от служителите става чрез получените потребителско име и парола.

Чл.36 Ползването на интернет и служебна електронна поща се ограничават съобразно скоростта на ползвания достъп до интернет, броя на откритите работни места и необходимостта от ползване на тези услуги съобразно служебните задължения на служителите.

Чл.37 Служителите на съответните работни места са длъжни да не споделят своите потребителски имена и пароли с трети лица и носят дисциплинарна отговорност, ако се установи неправомерно ползване на ресурсите на компютърната мрежа, достъпа до интернет или електронна поща при използване на предоставените им потребителски имена и пароли.

Чл.38 Компютрите, свързани в мрежата на ЦСОП“Св.св Кирил и Методий“ с.Кривня. използват интернет само от доставчик, с когото ППЕ има сключен договор за доставка.

Чл.39 Забранява се инсталирането и използването на комуникатори (като icq, skype и др. подобни), осигуряващи достъп извън рамките на компютърната мрежа на ЦСОП“Св.св Кирил и Методий“ с.Кривня. и създаващи предпоставки за

идентифициране на IP адрес на потребителя и за достъп на злонамерен софтуер и мобилен код до компютрите, свързани в компютърната мрежа на ЦСОП“Св.св Кирил и Методий“ с.Кривня..

Чл.40 Забранява се съхраняването на сървъра на ЦСОП“Св.св Кирил и Методий“ с.Кривня. на лични файлове с текст, изображения, видео и аудио.

Чл.41 Забранява се отварянето без контрол от страна на ръководител на направление ИКТ на:

1. получени по електронна поща или на преносими носители изпълними файлове, файлове с мобилен код и файлове, които могат да предизвикат промени в системната конфигурация, напр. файлове с разширения .exe, .vbs, .reg и архивни файлове;
2. получени по електронна поща съобщения, които съдържат неразбираеми знаци

РАЗДЕЛ V

ЗАЩИТА ОТ КОМПЮТЪРНИ ВИРУСИ И ДРУГ ЗЛОВРЕДЕН СОФТУЕР

Чл.42 С цел антивирусна защита се прилагат следните мерки:

1. всички персонални компютри имат инсталиран антивирусен софтуер в реално време, който се обновява ежедневно;
2. специалист ИКТ извършва следните дейности:
 - 2.1. активира защитата на съответните ресурси - файлова система, електронна поща и извършва първоначално пълно сканиране на системата;
 - 2.2. настройва антивирусния софтуер за периодични сканирания през определен период, но поне веднъж седмично;
 - 2.3. активира защитата на различните програмни продукти за предупреждение при наличие на макроси и настройва защитната стена на система;
 - 2.4. проверява за правилно настроен софтуер за автоматично обновяване на операционната система и инсталирания софтуер;
3. при поява на съобщение от антивирусната програма за вирус в локалната мрежа, всеки служител от съответното работно място задължително специалист ИКТ.

РАЗДЕЛ VI

НЕПРЕКЪСНАТОСТ НА РАБОТАТА

Чл.44 (1) Всички сървъри и устройства за съхранение на данни да са свързани към устройство за непрекъсваемост на ел. снабдяването.

(2) При липса на ел. захранване за повече от 10 мин. Специалист ИКТ започва процедура по поэтапно спиране на сървърите.

(3) При срыв в локалната компютърна мрежа, всеки потребител следва да запише файловете, които е отворил на персоналния си компютър, за да се избегне загуба на информация. При възстановяване на мрежата, всички локално запазени файлове следва да се преместят отново на сървъра и да се изтрият локалните копия.

Чл. 45 Инциденти, свързани с информационната сигурност се отстраняват съгласно :

1. Процедура за реакция при defacement на уебсайт – приложение №1;
2. Процедура за реакция при фишинг атака – приложение №2;
3. Процедура за реакция при заразяване със злонамерен софтуер – приложение №3.

Чл. 46 (1) За всеки инцидент в информационната система на ЦСОП“Св.св Кирил и Методий“ с.Кривня., който има въздействие върху непрекъснатостта на работа, ръководител на направление ИКТ уведомява екипа за реагиране при инциденти с компютърната сигурност към Държавната агенция „Електронно управление“ /контактни точки: 029492212, 0878908546, cert@govCERT.bg/. Първоначално уведомяване се прави до два часа след констатирането на инцидента. В срок до 5 работни дни се предоставя пълната информация за инцидента.

РАЗДЕЛ VII

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Служителите в ЦСОП“Св.св Кирил и Методий“ с.Кривня. са длъжни да познават и спазват разпоредбите на тези правила. Настоящите правила се включват в т.І на Декларацията за информираност, която попълват всички новопостъпили служители в ЦСОП“Св.св Кирил и Методий“ с.Кривня..

§ 2. Контролът по спазване на правилата се осъществява лично от директора.

§ 3. Настоящите вътрешни правила се разглеждат и оценяват периодически с оглед тяхната ефективност, като ЦСОП“Св.св Кирил и Методий“ с.Кривня. може да приема и прилага допълнителни мерки и процедури, които са целесъобразни и необходими с оглед защитата на информацията.

§ 4. Тези правила са разработени на основание чл.26 от Наредбата за общите изисквания за мрежова и информационна сигурност и са приети на педагогически съвет № 07 / 10.09.2024 год. и са утвърдени със заповед на директора на ЦСОП“Св.св Кирил и Методий“ с.Кривня .

Процедура за реакция при defacement на уебсайт:

Подготовка

1. Необходимо е да разполагате с актуални схеми, които описват компонентите на Вашия уеб сървър.
2. Необходимо е да разполагате с архив на уеб сайта, който при инцидент да заеме мястото на основния сайт и да стартирате процедура за пренасочване на посетителите към него.
3. Имплементирайте инструменти за мониторинг с цел бързо засичане на аномално поведение на Вашия уебсайт.
4. Експортирайте лог файловете на уеб сървъра на външен сървър (Log Management Server/ SIEM). Уверете се, че часовниците на сървърите са синхронизирани.
5. Ако Вашият уеб сайт се хоства от трета страна:
 - Поддържайте актуална информация за контакт с нея.
 - Уверете се, че тя прилага политика за събиране на логове за всички събития.
6. Уверете се, че имате актуална схема на мрежовата инфраструктура.
7. Поддържайте актуални контакти на всички, които участват в процеса на поддръжка системите - на доставчика на достъп до интернет, хостинг доставчика (ако уеб сайта не се хоства във Вашата инфраструктура), администратора на приложението, мрежовия администратор, nCERT България, ДАНС и ГДБОП.

Идентификация

1. Извършвайте мониторинг на уеб страницата с цел установяване кое съдържание е било променено.
2. Извършвайте проверки на сигурността на уеб сайта с инструменти като Google SafeBrowsing.
3. Уверете се, че наистина има defacement и определете неговия произход:
 - Проверете датите на модифициране на файловете и техните хешове.
 - Проверете mashup content providers.
 - Проверете линковете в уеб страницата (src, meta, css, script, ...).
 - Проверете лог файловете.
 - Сканирайте базите данни за зловредно съдържание.
4. Докладвайте за инцидента на
 - Ръководството
 - Фирмата, която поддържа системата, ако имат договор с такава
 - nCERT Bulgaria (до 2 часа съгласно закона за КС)
 - ДАНС, ако е обект със стратегическо значение
 - ГДБОП, ако има данни за киберпрестъпление

3. Проверете схемата на мрежовата инфраструктура. Уверете се, че уязвимостта, която е използвана, не се намира другаде.
 - Проверете системата, на която уеб сървърът работи.
 - Проверете какви други услуги работят на същата машина.
 - Проверете връзките с други системи и дали някоя от тях е компрометирана.
4. Ако източникът на атаката е друга система от мрежата, изключете я от мрежата, по възможност физически и я изследвайте.
5. Разберете коя техника е използвал атакуващия, коя е първоначално пробитата система и се опитайте да я поправите:
 - Уязвимост на уеб компоненти: поправете 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: променете правата за достъп.
6. Ако е необходимо при сложен проблем и много важен уеб сървър, вдигнете 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. Премахнете съдържанието, което е подменено и възстановете оригиналното.
2. Поправете намерените уязвимости.
3. Възстановете съдържанието, използвайки последния архив и се уверете, че съдържанието не съдържа уязвимости (ако уязвимите източници са от самите уеб приложения).
4. Прегледайте операционната система на уеб сървъра за подозрителни процеси и/или наличие на Backdoor/Rootkit и ги отстранете 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. Проверете за качен PHP Backdoor / Web Shell / Backdoor Shell чрез някой от

6. Променете всички потребителски пароли, ако уеб сървърът изисква потребителска автентикация и/или ако имате съмнения или доказателства за компрометирани акаунти.
7. Ако сте временно сте използвали архив на уеб сървъра (т.2 от Подготовка) , въведете основния обратно в експлоатация.
8. Документирайте подробно всяка стъпка от процеса на управление на инцидента
9. Използвайте комуникационна си стратегия ако defacement страницата е била видима за част от вашите потребители и планирайте да обясни публично инцидента.
10. Изгответе подробен доклад за инцидента и го направете достъпен за всички участващи страни. Той трябва да съдържа минимум:
 - Първоначално откриване;
 - Действия и срокове;
 - Какво се случи;
 - Какво се обърка;
 - Разходи за инциденти.
11. Изпратете подробния доклад на nCERT България до 5 дни след установяване на инцидента

Извлечени поуки / научени уроци от инцидента

- В случай на откриване на уязвимост, докладвайте за всички 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)
- Имплементиране на Web Application Firewall (в случай че няма)
- Имплементиране на IDS / IPS (в случай че няма) или настройка на правилата
- Имплементиране на File Integrity Monitoring
- Имплементиране на 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, Mail, DB Server, etc.)

Процедура за реакция при фишинг атака:

Е-мейл с линк към фишинг сайт

1. Проверете колко потребители в организацията са били подложени на фишинг атаката.
2. Определете дали лична или корпоративна информация е въведена във фишинг сайта.
3. Уведомете ръководството за възникналата ситуация, в зависимост от вътрешните правила във вашата организация.
4. Докладвайте за настъпилия инцидент на CERT България до 2 часа след неговото установяване.
5. След като неутрализирате атаката, анализирайте възникналата ситуация:
 - ✓ На база резултатите от събраната информация изгответе доклад относно вида и хронология на инцидента, предприетите мерки за разрешаването му.
 - ✓ Изгответе препоръки за предприемане на последващи проактивни мерки.
 - ✓ Разгледайте взетите решения и тяхната полза при фишинг атаката.
 - ✓ Извършете анализ какви ресурси са изразходвани при тази ситуация.
 - ✓ Помислете и над факта какви ресурси, било то външни или вътрешни, биха могли да ви помогнат при бъдещи подобни ситуации.
6. При необходимост обновете процедурата.
7. Изпратете подробен доклад на CERT България за причините, довели до фишинг атаката и предприетите действия.

Фишинг е-мейл с прикачен зловреден файл:

1. Проверете колко потребители в организацията са получили въпросния е-мейл.
2. Следвайте **Процедура за реакция при заразяване със злонамерен софтуер.**
3. Създайте групова политика (GPO) в Активната Директория забранете активиране и изпълнение на макроси в Microsoft Office.
4. Създайте 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.

Процедура за реакция при DDoS атака

8. Определете точките на отказ от услуги.
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.
9. Уведомете ръководството за възникналата ситуация, в зависимост от вътрешните правила във вашата организация
10. Докладвайте за настъпил инцидент на CERT България до 2 часа след неговото установяване.
11. Свържете се с вашия доставчик на интернет услуги за да уточните мащаба на DDoS атаката и нейното смекчаване.
12. Проверете дали всички устройства, сървъри и приложения са актуализирани до последна версия.
13. Ако не сте администратор на атакуваната система или устройства се свържете със съответния администратор.
14. Свържете с фирмата, поддържаща Вашите устройства, ако има такава.
15. Архивирайте логовете от всички засегнати устройства (сървъри, рутери, защитни стени и др.) и ги анализирайте, използвайки приложения за анализ на мрежовия трафик.
16. Създайте ACL за приоритизация на трафика.
17. Осигурете алтернативна комуникационна свързаност чрез VPN за критичните за Вас услуги.
18. Използвайте Reverse path forwarding (RPF).
19. Филтрирайте входящия и изходящия трафик.
20. Задайте лимити на:
 - скоростта на преминаващите ICMP пакет,
 - скоростта на преминаващите SYN пакет,
 - DNS TTL за атакуваните системи,

25. По възможност изключете всички неизползвани по време на атаката устройства.
26. Идентифицирайте и локализирайте DDoS трафика от реалния трафик.
27. При възможност използвайте геофилтриране.
28. Извършете контрол на content delivery на база на потребител и сесия.
29. Ако е възможно, преминете към алтернативна мрежа.
30. Ако атаката е към конкретно приложение, обмислете варианта временно да го спрете.
31. При възможност добавете допълнителни ресурси, като сървъри или мрежови устройства. Целта ви тук ще бъде да запазите услугата онлайн докато отстранявате проблема.
32. Извършвайте промените постепенно. При промяна изчакайте малко, за да разгледате ефекта от нея и при необходимост след това, въведете други промени.
33. Въведете филтри относно отговора на сървърите към DDoS трафика. Така ще филтрирате допълнително изпращане на пакети по мрежата ви.
34. След като неутрализирате атаката, трябва да анализирате възникналата ситуация:
 - ✓ Преценете какви предварителни действия можете още да предприемете.
 - ✓ Разгледайте взетите решения и тяхната полза при атаката.
 - ✓ Извършете анализ какви ресурси са изразходвани при тази ситуация.
 - ✓ Помислете и над факта какви ресурси, било то външни или вътрешни, биха могли да ви помогнат при бъдещи подобни ситуации.
35. При необходимост обновете процедурата.
36. Изпратете подробен доклад на CERT България за причините довели до атаката и предприетите действия.

Процедура за реакция при заразяване със злонамерен софтуер

1. Ако са заразени една или няколко системи, незабавно ги изключете физически от вътрешната мрежа, за да предотвратите разпространението на зловредния код и свързването им със C&C сървър.
2. Ако стъпка 1 не може да бъде извършена своевременно или са заразени значителна част от системите и не сте въвели силни защитни стени, изходни филтриращи и прокси сървъри, незабавно блокирайте ЦЕЛИЯ изходящ трафик към външни мрежи.
3. Уведомете ръководството за възникналата ситуация, в зависимост от вътрешните правила във вашата организация.
4. Докладвайте за настъпилия инцидент на CERT България до 2 часа след неговото установяване.
5. Конфигурирайте филтри на вътрешните мрежови устройства с цел изолиране на мрежови сегменти, в които има заразени системи. Наблюдавайте мрежовия трафик, за идентифициране на потенциални многостранни атаки.
6. Прегледайте подходящите лог файлове, за да се опитате да идентифицирате първата заражена система и какъв е векторът на атаката, ако е възможно.
7. От важно значение е да определите дали някоя от заразените системи успешно се свързва със сайт в Интернет, с който обменя информация.

- Да форматирайте твърдия диск и да възстановите системата.
- Да се уверите, че всички пачове, свързани със сигурността, са инсталирани.
- Да се уверите, че антивирусната ви програма е актуализирана до последна версия.
- Да промените паролите на локалните администратори и на потребителските акаунти за всички заразени системи.

10. Ако установите, че системата е заражена с малуер, направете следното:

- Да се уверите, че всички пачове, свързани със сигурността, са инсталирани.
- Да сканирате заразените машини, използвайки антивирусна система с дефиниции, за които е сигурно, че засичат съответния малуер.
- Да промените паролите на локалните администратори и на потребителските акаунти за всички заразени системи.

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

12. След като премахнете зловредния софтуер, анализирайте ситуацията:

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

13. При необходимост обновете процедурата.

14. Изпратете подробен доклад на CERT България за създалата се ситуация и предприетите действия.