ПРОФЕСИОНАЛНА ГИМНАЗИЯ ПО СТОПАНСКО УПРАВЛЕНИЕ, АДМИНИСТРАЦИЯ И УСЛУГИ „АТАНАС БУРОВ"– гр. СИЛИСТРА
7500 гр. Силистра, бул. „Македония" 121; тел./факс +359 86 821 859;
e-mail: economics_ss@abv.bg

ЗАПОВЕД

№ РД 09 – 398 /08.01.2019 г.

На основание чл. 259, ал. 1 от Закона за предучилищното и училищното образование, чл.31, ал.1, т.1 и т.6 от Наредба №15 от 2019г за статута и професионалното развитие на учителите, директорите и другите педагогически специалисти и Решение на общо събрание от 08.01.2020г.

УТВЪРЖДАВАМ:

План за действие при възникване на инциденти, свързани с информационната сигурност в ПГСУАУ „Атанас Буров" - Силистра.

1. Педагогическият и непедагогическият персонал от ПГСУАУ „Атанас Буров", са длъжни да спазват процедурите, описани в Плана за действие.
2. Определям отговорно лице за реагиране при възникване на инциденти г-жа Даринка Йорданова – ръководител направление ИКТ в ПГСУАУ „Атанас Буров".

Настоящата заповед да се сведе до знанието на целия педагогически и непедагогически персонал за изпълнение.

Контролът по заповедта възлагам на г-н Николай Колев – зам. директор АСД.

Денка Михайлова .....
Директор на ПГСУАУ „Атанас Буров"

УТВЪРЖДАВАМ:
Денка Михайлова - *Директор на ПГСУАУ „Атанас Буров"- гр. Силистра*

ПЛАН ЗА ДЕЙСТВИЕ

**при възникване на инциденти,
свързани с информационната сигурност
в ПГСУАУ „Атанас Буров", гр. Силистра**

Планът за действие е приет на Общо събрание с Протокол № 1/08.01.2020год. и е утвърден със Заповед №РД 09-398 /08.01.2020год. на директора на гимназията

Процедура за управление на инциденти, свързани с информационната сигурност

I. Цел на процедурата

Процедурата за управление на инциденти в ПГСУАУ „Атанас Буров" е тази, чрез която се определя начинът, 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 отреагира при какъвто и да е инцидент и да се намали неговото влияние върху организацията.

1. **Анализ на информационните активи и препоръки за повишаване на информационната сигурност**

1.1 Счетоводна програма - ползвател: главен счетоводител.

Стъпки за повишаване на информационната сигурност – да се извършва архив на данните периодично

1.2 Програмен продукт „Заплати" – ползвател: касиер.

Стъпки за повишаване на информационната сигурност – да се извършва архив на данните периодично – на външен хард диск

1.3 Програмен продукт „Хонорари"- ползвател: касиер.

Стъпки за повишаване на информационната сигурност – да се извършва архив на данните периодично – на външен хард диск

1.4 Електронна поща на училището - ползвател: технически сътрудник

Стъпки за повишаване на информационната сигурност – да се извършва архив на електронни писма, кореспонденции и папка със служебни документи ежемесечно – на външен хард диск или в облачно пространство.

1.5 Информационна система „АдминПро"– ползватели: Ръководител направление ИКТ, технически сътрудник

Стъпки за повишаване на информационната сигурност – съхраняване на резервно копие на сървър на Админ Софт, извършване на архив на данните периодично – на външен хард диск или в облачно пространство.

II. Роли и отговорности

ПГСУАУ„Атанас Буров" е внедрена подходяща организационна структура за управление на инцидентите – дефиниране на роли и отговорности. Одобрени са хората за контакт при инцидент, заедно с техните роли и отговорности. Всички са запознати с тях. Поддържа се 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. Списъкът се съхранява на достъпни места и на различни носители.

Последователност на действията при нарушаване на информационната сигурност:

1. Съобщаване за възникнал инцидент, свързан с информационната сигурност – работещият, установил инцидента, незабавно уведомява **Дарина Йорданова/РНИКТ/–тел: 0894493509**
2. Дарина Йорданова уведомява **Николай Колев /ЗДАСД/, тел: 0894493500** и директора на училището – **Денка Михайлова, тел: 0894419573**, изключва засегнатите системи от достъп, предприема действия за възстановяване на нормалната работа, при необходимост сформира екип за по-ефективно справяне със ситуацията.

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

Дейностите трябва да включват:

- ✓ Политиката за информационна сигурност и политиката за управление на риска са одобрени и разпространени;

- ✓ Определяне списък на възможните инциденти с вероятности за появяването им, изхождайки от оценките на риска;
- ✓ 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 център за възстановяване след инциденти (т.нар. "Disaster Recovery Center"), в който се извършва постоянно архивно съхранение ("back-up") на информацията от системата, така че да може да се възстанови нейната дейност след инцидента;

в) създаване на резервен изчислителен център, в който се поддържа репликирано състояние на критичните оперативно действащи системи, така че дейността им да бъде незабавно поета от него.

- ✓ Разработен и внедрен процес по установяване и докладване на възникнал инцидент, съгласно закона за киберсигурност;
- ✓ Разработен и внедрен процес по събиране на информация по определените събития;
- ✓ Разработен и внедрен процес по установяване и докладване на слабости и уязвимости в сигурността;
- ✓ Разработен и внедрен процес по определяне на всички засегнати външни и вътрешни ресурси на организацията;
- ✓ Разработен и внедрен процес по съхранение на събраните доказателства и техния интегритет;
- ✓ Разработен и внедрен процес по описване на действията извършени в процеса на управление на даден инцидент в съответната база.
- ✓ Определяне на критично важните функции на системата и установяване на приоритетите за възстановителни работи;
- ✓ Разработен и внедрен процес по поддръжка в актуално състояние на всички услуги предоставени от ПГСУАУ „Атанас Буров" и списък с използваните портове. Всички останали неизползваеми портове да бъдат забранени.
- ✓ Разработка на стратегии за възстановителни работи;
- ✓ Идентификация на ресурсите, необходими за изпълнение на критично важните функции;
- ✓ Разработен и внедрен процес по намаляване въздействието върху организацията;

IV. Цикъл на управлението на инциденти

Той трябва да 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 примерни 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 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;
- Докладване за инцидент съгласно процедурата на ръководството, на nCERT Bulgaria, на ДАНС, ако е обект със стратегическо значение 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;
- 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;

V. Актуализация на процедурата, ако е необходимо

VI. Утвърждаване на процедурата

Приложение 1

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 анормално 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

Ограничаване на въздействието

1. Изключете компрометираният сървър от мрежата
2. Направете 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. 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 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. 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 defeicment 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 Vuln, DB Server Vuln и т.н.)

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.
5. Повтарят се стъпки след точка 5 от предната

Приложение 2

Процедура за реакция при DDoS атака

1. 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.

2. Уведомете ръководството за възникналата ситуация, в зависимост от вътрешните правила във вашата организация

3. Докладвайте за настъпилия инцидент на CERT България до 2 часа след неговото установяване.

4. Свържете се с вашия доставчик на интернет услуги за да уточните мащаба на DDoS атаката и нейното смекчаване.

5. Проверете дали всички устройства, сървъри и приложения са актуализирани до последна версия.

6. Ако не сте администратор на атакуваната система или устройства се свържете със съответния администратор.

7. Свържете с фирмата, поддържаща Вашите устройства, ако има такава.

8. Архивирайте логовете от всички засегнати устройства (сървъри, рутери, защитни стени и др.) и ги анализирайте, използвайки приложения за анализ на мрежовия трафик.

9. Създайте ACL за приоритизация на трафика.

10. Осигурете алтернативна комуникационна свързаност чрез VPN за критичните за Вас услуги.

11. Използвайте Reverse path forwarding (RPF).

12. Филтрирайте входящия и изходящия трафик.

13. Задайте лимити на:

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

14. Търсете модели на трафика, за да идентифицирате познати атаки.

15. Разберете дали сте обект на атаката или косвена жертва.

16. Идентифицирайте атакуващите IP адреси и ги проследете в лог файловете, за злонамерени действия преди началото на атаката.

17. Сканирайте устройствата за зловреден софтуер, влязъл при атаката.

18. По възможност изключете всички неизползвани по време на атаката устройства.

19. Идентифицирайте и локализирайте DDoS трафика от реалния трафик.

20. При възможност използвайте геофилтриране.

21. Извършете контрол на content delivery на база на потребител и сесия.

22. Ако е възможно, преминете към алтернативна мрежа.

23. Ако атаката е към конкретно приложение, обмислете варианта временно да го спрете.

24. При възможност добавете допълнителни ресурси, като сървъри или мрежови устройства. Целта ви тук ще бъде да запазите услугата онлайн докато отстранявате проблема.

25. Извършвайте промените постепенно. При промяна изчакайте малко, за да разгледате ефекта от нея и при необходимост след това, въведете други промени.

26. Въведете филтри относно отговора на сървърите към DDoS трафика. Така ще филтрирате допълнително изпращане на пакети по мрежата ви.

27. 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.

28. При необходимост обновете процедурата.

29. Изпратете подробен доклад на CERT България за причините до довели до атаката и предприетите действия.

Приложение 3

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 сървъра.
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 заразена 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.
8. Извършете forensic анализ на системата, идентифицирана в стъпка 6, за да определите обсега на компрометиране и да предприемете подходящите действия за премахване на зловредния код. Не се доверявайте на вече инсталирания на системата софтуер, защото и той също може да е компрометиран.
9. Ако установите, че е инсталиран rootkit, за всяка заразена система, направете следното:

- Да се уверите, че имате backup на важните данни.
- Да форматирате 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 заразена 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.

Лица

за контакт при възникнал инцидент

№	Име, фамилия	Длъжност	Отговорност	Подпис
1	Николай Крумов	Зам.директор АСД		
2	Дарина Йорданова	РНИКТ	ИС „АдминПро"	
3	Даниел Крумов	Гл. счетоводител	Счетоводна програма	
4	Искра Маринова	Касиер	Програмни продукти „Заплати", „Хонорари"	
5	Цветанка Неделчева	Технически сътрудник	Електронна поща	