

Указания за повишаване мрежовата и информационна сигурност на предстоящите избори на 25.10.2026 г.

Тема: Указания за повишаване мрежовата и информационна сигурност на предстоящите избори на 25.10.2026 г.

От: "CERT" <cert@govcert.bg>

Дата: 22.10.2026 г., 10:46

До: "CERT" <cert@govcert.bg>

Здравейте,

Във връзка с предстоящите избори за президент и вицепрезидент на 25.10.2026 г. Ви изпращаме указания с необходимите мерки за повишаване нивото на мрежова и информационна сигурност.

С уважение,

CERT България

E-mail: cert@govcert.bg

Tel: +359 2 949 2212

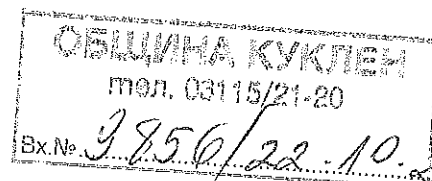
Mobile: +359 878 908 546

Web: www.govcert.bg

Прикачени файлове:

Указания за МИС-2026_izbori.docx

48,9 KB



УКАЗАНИЯ

за повишаване нивото на мрежовата и информационната сигурност

Във връзка с предстоящите изборите за президент и вицепрезидент на републиката на 25 октомври 2026 г., насрочени с решение на Народното събрание, публикувано в ДВ брой 70 / 2026 г., в съответствие с чл. 12, т. 3 от Закона за киберсигурност (ЗКС) и с мерките, предвидени в Наредбата за минимални изисквания за мрежова и информационна сигурност (НМИМИС), Ви напомняме, че съгласно чл. 21, ал. 1 от ЗКС, административните органи осигуряват и отговарят за сигурността на използваните от тях мрежи и информационни системи, като основните задължения и изисквания по отношение на мрежовата и информационна сигурност се съдържат и в НМИМИС. Съгласно чл. 3, ал. 1, т. 1 от същата наредба, административният орган, съответно ръководителят на субекта, носи пряка отговорност за информационната сигурност в обхвата на наредбата, дори и когато дейността е възложена за изпълнение на трети страни.

В тази връзка Ви препоръчваме да предприемете необходимите долуизложени мерки за повишаване нивото на мрежовата и информационната сигурност, съдържащи се в съществуващите нормативни документи:

1. Уверете се, че е преустановена работата на техническите средства и системи, които не са от съществено значение за обезпечаване на изборния процес

2. Извършете проверка на отговорните лица, които административират и модерират официалните страници в социалните мрежи, използвани за комуникация с обществеността

3. Актуализирайте схемите на ИТ инфраструктурата и описа на информационните активи

Актуализацията е от съществено значение за документиране на настоящото състояние и разкриване на неизвестните и неodobрени активи, включени в мрежата, на уязвимости в софтуера, на слабости в инфраструктурата, като например единични точки на отказ, неправилна сегментация на мрежите и пропуски в конфигурациите, които увеличават риска от кибератаки. Схемите на ИТ инфраструктурата и описа на информационните активи ще Ви помогнат при взимане на информирани решения в случай на инциденти със сигурността.

4. Направете основен преглед на дейностите и услугите, които предлагате чрез ИТ инфраструктурата на Вашата администрация

Идентифицирайте информационните активи, които участват в отделните дейности на администрацията и предоставянето на всяка услуга. Приоритизирайте дейностите и услугите, за да вземате бързо решения в случай на киберинцидент. Проверете до каква степен са обвързани инфраструктурите, предоставящи вътрешни и външни услуги и преценете как би повлияла евентуална кибератака на едните или на другите. Сегментируйте различните услуги, така че при атака и компрометиране на една от тях, другите да не бъдат засегнати. Особено внимание обърнете на всички услуги, които са презентирани в Интернет, като например web сайтове, портали, електронна поща, VPN достъп и др. Спрете достъпните от интернет услуги и сайтове, които са в режим на тестване и разработка. **Не изключвайте** услуги, сайтове и портали, които са важни за функционирането на администрацията Ви, а вземете мерки за тяхната защита.

5. Идентифицирайте кой осъществява поддръжка и администриране на ИКТ системите, обезпечаваша дейностите и предоставящи услугите.

Независимо дали поддръжката и администрацията се осъществява от Ваши служители и/или външни организации, идентифицирайте цялата верига на доставчици за Вашите онлайн услуги, за да може адекватно да ги защитите. Изискайте от доставчиците да гарантират, че прилагат механизми за постигане на високо ниво на мрежова и информационна сигурност.

6. Поддържайте актуален списък с контакти на всички, от които зависи дейността и услугите, които предоставя администрацията Ви:

Съгласно добрите практики, с цел способност за своевременна реакция е препоръчително да сте създали и да поддържате актуален списък с контакти на всички, от които зависи дейността и услугите, които предоставяте. Ваши служители и външни фирми, отговарящи за поддръжката и администрацията на системи, приложения и мрежови устройства, както и доставчиците Ви на достъп до Интернет.

7. Ако не разполагате със специализирано оборудване за защита от DDoS кибератаки, консултирайте се с Вашите доставчици на достъп до Интернет какви контрамерки са предприели или могат да предприемат срещу кибератаки, включително и (D)DoS такива. Ако е необходимо и възможно, коригирайте договорите си с тях, като се включат и техни задължения при кибератаки.

Във взаимоотношенията си с доставчиците задължително трябва да уточните:

- какви са контактните точки при кибератаки;
- какви механизми използват доставчиците за ранно откриване на кибератаки;
- какви контрамерки са в състояние да предприемат за смекчаване на атаката и какви биха били евентуалните последици от тях;
- какви контрамерки използват, за да Ви защитят от атаки, насочени към други техни клиенти;
- с какъв тип организации споделяте инфраструктурата в случай на споделен хостинг;
- прилага ли се инсталиране на актуализации за защита (security updates, patches).

8. Изискайте от специалистите от Вашето ведомство и от външните фирми, отговарящи за поддръжката и администрацията на системи, приложения и мрежови устройства, да направят преглед на мерките, които са взети за защита на всяко приложение, сървър и мрежово устройство от Вашата ИК инфраструктура, включително и на конфигурациите им. При необходимост да се предприемат допълнителни организационни и технически мерки, за да са по-устойчиви на кибератаки.

9. Проверете дали антивирусните програми работят с актуални бази с данни от вирусни дефиниции (дали се обновяват редовно), какви предупреждения издават и какво е предприето въз основа на тях.

10. Проверете дали са приложени последните актуализации, отстраняващи уязвимости в сигурността на използваните от вас 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 Вашето ведомство. Обърнете особено внимание на използвания безплатен софтуер и този с отворен код, като например Linux базирани операционни системи, Apache, BIND, OpenSSL, PHP, Network Time Protocol Daemon и др. Уязвимостите в софтуера и фърмуера се използват за осъществяване на кибератаки, включително и срещу други организации. Организирайте регулярно да се проверява за нови актуализации, отстраняващи

уязвимости в сигурността, на страниците на съответните производители, www.cvedetails.com или на www.govcert.bg.

11. Направете преглед на достъпите – проверете дали всички потребители, на които е даден достъп до ведомствената Ви мрежа, до отделните системи и приложения, имат право на него в съответствие със служебните им задължения: дали външни лица имат достъп (бивши служители, представители на външни организации); проверете какви права са дадени на всеки, като обърнете особено внимание на административните акаунти и тези с привилегии. Изискайте информация за наложените политики за управление на паролите – на какъв период се сменят, каква е сложността им, кога последно са променяни паролите. Паролите трябва да се променят периодично, но най-малко веднъж на 6 месеца. Достъпите трябва да са индивидуални, а не групови или споделени. В ежедневната работа трябва да се използват акаунти с най-ниско ниво на достъп. Не трябва да има потребители с неизтичащи пароли и с пароли, които не отговарят на минималните изисквания за комплексност, тъй като те могат да бъдат използвани за компрометиране на инфраструктурата Ви. Особено внимание обърнете на отдалеченият достъп до инфраструктурата – този достъп трябва да е разрешен само по необходимост, да бъде осъществяван чрез VPN (виртуална частна мрежа), като **не са допустими** използването на технологии като RDP, VNC и др., особено презентирани в Интернет.

12. Делегирайте администраторски права на акаунти с по-ниски нива на привилегии

Администраторските акаунти с най-високо ниво на привилегии като „administrator“ и „root“, трябва да бъдат използвани само и единствено в случаите, когато това е напълно необходимо, а не за ежедневна работа. Добра практика за управлението на администраторски акаунти с най-високо ниво на привилегии е акаунтите да делегират определени правомощия на конкретни второстепенни акаунти с по-ниско ниво на привилегии, които в ежедневната работа ще бъдат използвани за конкретни дейности. По този начин се намалява риска от компрометиране на администраторския акаунт с най-високи привилегии.

Например, управлението на (потребителски) акаунти съгласно тази практика означава, че администрирането на (потребителските) акаунти ще се извършва от акаунт, на който са били делегирани права от администраторския акаунт с най-високи привилегии, така че администраторският акаунт с най-високи привилегии повече да не бъде използван за тази цел.

Проверете всички акаунти с високо ниво на привилегии и се уверете, че всеки акаунт все още е нужен, че служителят, който го ползва, е на работа и има нужните компетенции за работата по поддръжка и управление на системите. В случай, че паролата на тези акаунти не е сменяна последните 6 месеца – иницитирайте смяна на паролата, като не забравяте минималните изисквания за комплексност.

13. Проверете дали регулярно се извършва резервиране и архивиране на информацията, тъй като е критично важна за поддържане на непрекъсваемостта на дейността на администрацията и услугите, които предоставя. Проверете дали резервните копия се съхраняват надеждно и дали са годни за употреба. Архивните копия трябва да бъдат **недостъпни онлайн**, като не се допуска извършване на архивиране на същите дискове и системи, на споделено по мрежата устройство за съхранение и на постоянно свързани USB дискове. Архивирането трябва да се извършва регулярно – най-малко веднъж седмично и по-често – по усмотрение на ръководството на организацията. Това е основна мярка за защита срещу ransomware атаки, при които обикновено се компрометира цялата домейн инфраструктура и всички потребители. Поддържането на недостъпно онлайн копие и/или

изключено от мрежата средство за съхранение на архивирана информация (например на лента за съхранение) създава възможност за възстановяване на функционирането на администрацията дори и при такава атака.

Пример за създаване на план за подобно архивиране би бил: създаване на инкрементални архиви всеки ден, които се съхраняват на бекъп сървър. Създадените седмични пълни архиви се съхраняват на бекъп сървър, намиращ се в резервен център или при доставчик на услуги, а поне един пълен месечен архив се съхранява на отделен носител, заключен в огнеупорна каса.

Минимум веднъж годишно трябва да се провежда тренировка по възстановяване на информация от архивно копие, като по този начин се целят две неща: тренировката и придобиване на опит на служителите при възстановяване на информация от архив и проверка на работоспособността на архивните копия. В случай че за последната година не сте извършвали такава тренировка – планирайте я и я осъществете преди датата на изборите.

14. Проверете актуалността на установените във Вашето ведомство вътрешни правила за мрежовата и информационната сигурност, процедури и правила за реакция при инциденти. Ако нямате такива, създайте и въведете вътрешни правила в организацията, утвърдени от ръководството. При създаването на тези правила е най-важно да бъдат идентифицирани съответните заинтересовани страни в различните сценарии, техните отговорности и способности за комуникация. С правилата трябва да са запознати всички Ваши служители и партньори, участващи в поддръжката и администрацията на ИК инфраструктурата.

15. Направете планове за действие при инциденти, включително и в случай на кибератака, в които трябва да е ясно установено:

- кой е отговорен за организацията при подобна ситуация;
- кой, кого, кога ще информира (функционална и йерархична ескалация);
- кой и какво ще предприеме при първоначалното установяване на атаката, при установяване на мащаба на засегнатите системи и при ограничаването на щетите;
- кой и с кого ще се консултира, какви договори за поддръжка има активни (използвайте информацията от т.4);
- кой ще събира и съхранява необходимата информация и т.н;
- кой, кога и каква информация ще сподели със служители, доставчици, клиенти, медии, държавни органи.

Помислете за алтернативни канали за комуникация, за да не останете в информационна изолация при такава ситуация.

Не забравяйте, че съгласно чл. 21, ал. 3 от Закона за киберсигурност административните органи уведомяват Националния екип за реагиране при инциденти с компютърната сигурност (НЕРИКС), изпълняващ функциите на секторен екип за реагиране при инциденти с компютърната сигурност за административните органи, създаден към МИДТ, за инцидентите, които имат въздействие върху непрекъснатостта на тяхната дейност (контактни точки: 24/7: 0878 908 546, cert@govCERT.bg).

14. Организирайте наблюдение на входящия и изходящия мрежови трафик и на натоварването на важните устройства за ИК инфраструктура спрямо установените нормални стойности на параметрите. Това означава периодично измерване и анализ на параметрите и сравняването им с нормалните стойности. Наблюдението дава възможност за ранно откриване на атаката, спомага при анализа ѝ и подпомага вземането на мотивирано

решение за предприемане на ефективни действия за противопоставяне. Атаките обикновено биват предхождани от сканиране за откриване на уязвимости в софтуера и конфигурациите.

16. Актуализирайте инструкциите към Вашите служители относно киберхигиена, прилагайте добри практики за мрежова и информационна сигурност, включително и за социалните платформи като Facebook, Instagram, LinkedIn, YouTube, X (бивше Twitter) и др., като:

Когато проверяват своята електронна поща да бъдат внимателни с прикачените файлове и линковете в писмата. Ако има прикачен файл, винаги първо да проверяват дали подателят е автентичен и дали има логика подателят да им изпраща подобен прикачен файл. В случаите, когато служителите получат съмнителна електронна поща, е препоръчително да проверят автентичността на изпращача и дали наистина е автор на съответното съобщение или файл. Те могат да проверят чрез друг начин на комуникация, различен от този, по който са получили подозрителното известие, напр. като се обалят по телефона и поискат потвърждение от предполагаемия автор. Ако е бил изпратен линк, винаги първо да го копират и проверяват на сайт за сканиране за вируси преди да го последват (например: <https://www.virustotal.com>). В случаите, когато служител се е подвел и е отворил съмнителен файл или е предоставил потребителското си име и парола на потенциален фишинг сайт, то той незабавно трябва да се свърже със служителя или административното звено, отговарящо за мрежовата и информационна сигурност и да се предприемат незабавни действия за определяне на обхвата на щетите, които могат да произлязат от инцидента, както и да бъдат предприети пропорционални на заплахите действия за ограничаване на щетите от него.

- Ако забележат забавяне на бързодействието на устройството им при посещение на определен сайт, да затворят сайта и да уведомят служителя, отговарящ за мрежовата и информационна сигурност, и да не го посещават. Някои сайтове се възползват от процесорната сила на своите посетители, като поддържат на страниците си скриптове за “копаене” на криптовалути, като не във всички случаи антивирусните програми са способни да засекат подобна кражба на ресурси.

- Задължително е използването на силна и сложна парола – трябва да включва главни и малки букви, цифри и специални символи; не трябва да съдържа лични данни като име, дата на раждане, телефонен номер и други, както и последователни цифри или букви. Препоръчва се същата парола да не се използва и за други акаунти. За гарантиране на висока степен на защита паролата следва да бъде регулярно променяна, при спазване на правилата за комплексност. Не споделяйте и не оставяйте паролата написана в явен вид на достъпни и за други лица места;

- Включете двуфакторна автентикация, за да добавите допълнително ниво на сигурност към акаунта Ви. Това може да включва изпращане на код на мобилния Ви телефон или използване на приложения за генериране на кодове;

- Създаденият с цел администриране на страницата на държавния орган акаунт да не се използва за лични цели, а само за нарочените такива;

- За обезпечаване непрекъснатостта на контрола на поддържания профил, същият следва да има двама администратори с възможност за взаимозамменяемост;

- При създаване на акаунт използвайте подход със задаване на минимални права (принцип на най-малките привилегии), достатъчни за изпълнение на предвидените задължения с цел минимизиране на евентуалните последствия при компрометиране на профила. Това означава, че трябва да дадете само тези права, които са необходими за изпълнението на задачите на потребителя;

- Редовна проверка на правата за достъп на акаунта и премахване на приложенията и потребителите, които не са свързани с дейността на администрацията;

- Използването на публични Wi-Fi мрежи крие рискове и представлява потенциална опасност за компрометиране на акаунта, затова при необходимост от използване на такива,

като мярка за сигурност използвайте виртуална частна мрежа (VPN) за шифроване на данните си, което ще Ви предпази от кибератаки, като например MITM (man-in-the-middle) атаки;

- Повишено внимание при отваряне на линкове, особено тези, които са непознати за Вас. Не следвайте линкове, които изглеждат подозрителни. По възможност използвайте допълнителен канал за потвърждение от страна на изпращача. Като основна мярка за проверка винаги сравнявайте посочения URL адрес, който се визуализира в hint полето в долния ляв ъгъл на брауъра;

- По отношение на официалната комуникация осигурете конфиденциалността, целостта и верността на информацията, като спазвате утвърдените Методически указания за формиране наименованията на домейните и поддомейните, както и на адресите на електронната поща на административните органи в Република България в съответствие с чл. 47 от Наредбата за общите изисквания към информационните системи, регистрите и електронните административни услуги, приета с постановление № 3 на Министерския съвет от 2017 г. (дв. бр.5 от 2017 г.). Моля, имайте предвид, че използване на пощенски платформи на трети страни могат да бъдат рискови за административния орган и да доведат до разкриване на държавна, конфиденциална или лична идентифицираща информация (по смисъла на GDPR). В случай че Вашата организация не разполага с необходимите ресурси за изпълнение на нормативния критерий, можете да заявите услугата „WEB електронна поща“, описано на сайта на МИДТ на: <https://e-gov.bg/wps/portal/agency/infrastructure/apps> чрез следната Форма за заявяване на услуга „WEB електронна поща“. Услугата „WEB електронна поща“ се предоставя безвъзмездно и осигурява всички функции и стандарти, отговарящи на съвременните изисквания за високо ниво на киберсигурност. Услугата може да се използва както в поддомейн на домейн **egov.bg**, така и в съществуващ публичен интернет домейн – регистриран на името на администрацията, като включва функции като антивирусни и антиспам опции за интеграция, възможности за използване през мобилни устройства и поддръжка на Exchange ActiveSync;

- Да се инсталират приложения само от официалните магазини на операционната система на съответното устройство, за да се избегне опасността от инсталиране на зловреден софтуер, който може да навреди на устройството или да открадне лични данни. В официалните магазини на операционните системи приложенията се проверяват предварително за зловреден код и други рискове;

- На устройство, чрез което се достъпва акаунт на държавна структура в социална платформа, да не се инсталират непроверени приложения, които не са предоставени от официалните магазини на операционната система на съответното устройство, както и такива със спорна репутация по отношение на международни политически отношения;

Препоръчителни планове за действие при киберинциденти

1. При атака от тип „отказ от услуга“ (DDoS)

В случай на смущения в работата на вашите информационни системи е препоръчително да бъдат предприети следните стъпки:

Стъпка 1: Определете дали смущенията се дължат на DDoS атака или има друга причина.

Проблем с неправилно конфигуриране на DNS, проблеми с рутирането и човешка грешка са също често срещани причини за прекъсване на мрежата. Колкото по-бързо проверите дали прекъсването е причинено от DDoS атака, толкова по-бързо можете да реагирате.

- Проверете изходящите връзки. Ако няма изходящи връзки, то атаката е толкова силна, че блокира целия входящ и изходящ трафик. Направете проверка с обичайните си инструменти за диагностика (като *traceroute*, *ping* и *dig*), за да изключете всички такива възможности.

- Проверете достъпа по IP адрес и по url до вашите онлайн услуги от външни мрежи.

- Проверете логовете на различни мрежови устройства и сървъри, участващи в предоставянето на засегнатата услуга. Логовете трябва да се съхраняват на отделна машина за период от минимум седем дни. Ако се налага, архивирайте ги и имайте готовност да ги предоставите на оторизирани органи при поискване.

Стъпка 2: След като се установи, че става въпрос за атака, трябва да се свържете с:

- ръководителите на екипите (Ваши служители или външни фирми), отговарящи за поддръжката и администрацията на системите, приложенията и мрежовите устройства.:

- Вашите доставчици на Интернет услуги – могат да потвърдят атаката; да предоставят информация кои други клиенти биха могли да бъдат засегнати от атаката; да предложат механизми за смекчаване.

Стъпка 3: Вземете 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.

Стъпка 4: Определете естеството на атаката

Първият въпрос, на който трябва да се отговори, е „Какви са векторите на атака?“

Опитайте се да определите дали атаката е:

- Обемна (Volumetric) – основаваща се на „наводнение“ (flood-based), която може да бъде на нива 3,4 или 7 от OSI модела;

- Асиметрична (Asymmetric) – предназначена е да предизвиква временни прекъсвания (timeouts) или изменения в състоянието на сесията (session-state);

- Изчислителна (Computational) – предназначена да консумира ресурси на процесорите и паметта;

- Основана на уязвимости (Vulnerability-based) – предназначена да използва софтуерни уязвимости.

Стъпка 5: Направете оценка на възможностите за смекчаване на атаката чрез въздействие на IP адресите на източниците на трафика.

Определете колко са източниците на атака:

- Ако списъкът на атакуващите IP адреси е малък, можете да ги блокирате на защитната стена. Всеки адрес, който добавите към списъка за блокиране, може да забави обработката и ще увеличи натоварването на процесора.

- Ако списъкът на атакуващите IP адреси е твърде голям, трябва да определите регионите, към които принадлежат, и тогава Вие или Вашия доставчик на Интернет можете да приложите т.нар. геоблокиране.

Стъпка 6: Смекчаване на специфични атаки към приложения

Ако блокирането на IP адреси на източника е неефективно, то DDoS атаката вероятно е на приложно ниво от OSI модела. Тези атаки изглеждат като нормален трафик на слой 4 от OSI модела, но създават аномалии, които нарушават услуги в сървъра, в заявките или обръщенията към бази данни. Атаките може да бъдат реализирани чрез:

- „наводнение“ от рекурсивни GET заявки;
- повтарящи се заявки за някои по-големи обекти (като например MP4 или PDF файли);
- повтарящи се заявки за обръщения към база данни.

За борба с тези атаки трябва да разрешите или да се изградят защитни механизми на ниво приложения и достъп до приложения.

Добра защита срещу такива атаки са следните техники, които зависят от възможностите на Вашето приложение и трябва да са предварително подготвени:

- login wall - логическа защита, която изисква потребителят да се впише в профил, който е предварително известен. Тази защита може да бъде приложена на нивото на доставчика на услуги, защитна стена на уеб приложение.
- Human detection - е вторият най-добър подход. Валидиране, че клиентската връзка се контролира от човека, а не от зловреден бот. Обикновено това се прави с CAPTCHA.
- Real browser enforcement - някои защитни стени на уеб приложение предоставят тази функционалност чрез вмъкване на JavaScript за пренасочи към нови връзки и след това ги записват в черен списък, ако те не следват пренасочването. Това е полезен подход, защото това блокира по-голямата част от ботове без да засяга реални потребители, използващи реални браузъри.

III. При атака от тип „ransomware“/криптовирус

Атака от този тип представлява процес, който криптира част от/или всички файлове на заразената машина и се визуализира съобщение за искане на откуп, за да ги декриптира.

Можете да разпознаете атака от тип “ransomware” по един или няколко от следните симптоми:

- Подмяната на wallpaper с изображение на искане за откуп;
- Появата на текстови файлове с искане за откуп;
- Появата на множество файлове с еднакво разширение, което не разпознавате (например .ecc, .ezz, .exx, .zzz, .xyz, .aaa, .abc, .ccc, .vvv, .xxx, .ttt, .micro, .encrypted, .locked, .crypto, _crypt, .crinf, .r5a, .XRNT, .XTBL, .crypt, .R16M01D05, .pzdc, .good, .LOL!, .OMG!, .RDM, .RRK, .encryptedRSA, .crjoker, .EnCiPhErEd, разширения от 6-7 случайни символи и др.);
- Спиране на работата на информационни системи и услуги вследствие на недостъпни файлове.

В случай на Ransomware е препоръчително да бъдат предприети следните стъпки:

1. Незабавно изключете достъпа до Интернет на цялата мрежа – чрез изключване на рутер и/или издърпване на мрежови кабели.
2. Незабавно прекъснете работата на мрежата или мрежите – чрез физическо изключване на мрежовите кабели, изключване на комутатори и маршрутизатори и др. Да се изключат безжичните системи, като рутери и AP.
3. Изключете и извадете всички външни устройства за съхранение на данни – флаш памети, външни дискове и др.
4. В случай че идентифицирате системи, които не са засегнати или са в процес на криптиране – незабавно ги изключете, като използвате хардуерен подход: издърпване на захранващ кабел, превключвател на захранване или натискане и задържане на бутона за захранване. По този начин ще се спре процесът по криптиране и ще се запази поне част от информацията.
5. В никакъв случай **НЕ ЗАПОЧВАЙТЕ** процеса по възстановяване от архивни копия, преди да сте сигурни, че мрежата е изчистена от зловреден код и векторът на проникване е елиминиран.

6. Опитайте се да идентифицирате с кой конкретен вариант на зловреден код от типа ransomware сте били заразени, като следвате инструкциите на адрес:

<https://www.nomoreransom.org/crypto-sheriff.php>

Ако успеете да идентифицирате използвания вариант на зловреден код, моля изпратете и тази информация на НЕРИКС.

7. След свързване с НЕРИКС ще получите инструкции за по-нататъшни действия за ограничаване на въздействието на инцидента и възстановяване на работоспособността на системите.

8. Не плащайте искания откуп. В много от случаите декриптирането на файловете не е възможно и ще понесете двойни щети: за откупа и за експертна помощ за възстановяване на информацията, като и в двата случая няма гаранция за постигане на положителен резултат.

ИЗИСКВАНИЯ ЗА ДОКЛАДВАНЕ

Съгласно чл. 21, ал. 3 от Закона за киберсигурност, административните органи уведомяват националния екип за реагиране с компютърната сигурност (НЕРИКС), изпълняващ функциите на секторен екип за реагиране при инциденти с компютърната сигурност за административните органи, създаден към МИДТ, за инцидентите, които имат въздействие върху непрекъснатостта на тяхната дейност:

- първоначално уведомяване - до 24 часа след констатиране на инцидента;
- в срок до 1 месец, като се предоставя пълната информация за инцидента.

За целите на докладването следва да се използва Приложение №7 към чл. 31, ал. 2 от Наредбата за минималните изисквания за мрежова и информационна сигурност (НМИМИС).

Контактни точки на НЕРИКС:

24/7: Моб. тел. : 0878 908 546

Тел. : +359 2 949 2212;

Електронна поща: cert@cert.bg

ВАЖНО Е ДА ЗНАЕТЕ!

За съдействие от НЕРИКС и/или други специализирани органи при разследване на инцидент/атака е необходима следната информация, като е задължително да изпратите установените артефакти за анализ:

- времеви период на атаката включително начало и край;
- размер на пакетите, брой на пакети в секунда и на използваната честотна лента при DDoS атака;
- протокол (ICMP, DNS, TCP, UDP, и т.н.);
- IP адреси и портове както на източника така и на целта;
- URL адрес на целта;
- HTTP хедъри (user-agent, language, encoding и т.н.);
- трафик на данните и информация за рутирането, например BGP;
- какви мерки са предприети за смекчаване на въздействието на атаката;

Мерките за защита срещу кибератаки са препоръчителни и само част от възможните, подготвени със съдействието на НЕРИКС на други държави-членки на ЕС и НАТО и на Агенцията на Европейския съюз за киберсигурност – ENISA.

При необходимост от допълнителна информация може да се обръщате към НЕРИКС на горепосочените контакти.