УСТОЙЧИВОСТ НА КИБЕРСИГУРНОСТТА НА ДЪРЖАВНАТА И МЕСТНАТА АДМИНИСТРАЦИЯ ПРИ БЕДСТВИЯ, АВАРИИ И КАТАСТРОФИ

професор д.т.н. Веселин Целков
Университет по библиотекознание и информационни технологии

асистент д-р Георги Средков
Югозападен университет „Неофит Рилски“, Благоевград

CYBERSECURITY RESILIENCE OF STATE AND LOCAL ADMINISTRATION IN DISASTERS, ACCIDENTS AND CATASTROPHES

Prof. DSc Veselin Tselkov
University fir Library Studies and Information Technologies

Assist. Prof. PhD Georgi Sredkov
South-West University „Neofit Rilski” – Blagoevgrad

Abstract: *The cybersecurity resilience of state and local administration is a critical aspect of their disaster response preparedness in today's interconnected world. As disasters, accidents and catastrophes can have a significant impact on communities and public services, ensuring the security and integrity of digital infrastructure is increasingly important to the normal functioning of the government. This publication shares some key considerations and measures to improve cyber resilience.*

Key words: *cybersecurity, resilience, administration, disasters, accidents, catastrophes*

Устойчивостта на киберсигурността на държавните и местните администрации е критичен аспект в тяхната готовност за реакцията при бедствия в днешния взаимосвързан свят. Тъй като бедствията, авариите и катастрофите могат да имат значително въздействие върху обществените услуги, гарантирането на сигурността и целостта на цифровата инфраструктура става все по-важно за нормалното функциониране на държавата. Ето някои ключови съображения и мерки за подобряване на киберустойчивостта:

- **Оценка на риска и планиране:** Държавните и местните администрации трябва да извършват цялостни оценки на риска, за да идентифицират потенциални кибер заплахи и уязвимости. Това включва анализ на въздействието на бедствията върху критичната инфраструктура и основните услуги, както и оценка на устойчивостта на съществуващите мерки за киберсигурност.
- **Резервиране и архивни копия:** Прилагането на резервиране и редовно архивиране на данни са от съществено значение, за да се гарантира, че критичните системи могат да продължат да работят дори при кибератаки или инфраструктурни повреди, причинени от бедствия. Архивирането на данни извън основния обект е особено важно за защита срещу физически щети на местната инфраструктура.

- **Обучение и осведоменост за киберсигурност:** На персоналът, работещ в държавните и местните администрации, трябва да се провежда редовно обучение за киберсигурност, за да идентифицира и реагира ефективно на киберзаплахи.
- **Планиране на реакция при инциденти:** Разработването и тестването на специализиран план за реагиране при инциденти, свързани с киберсигурността по време на бедствия, е от решаващо значение. Този план трябва да очертава ролите, отговорностите и действията, които да се предприемат в случай на кибер инцидент и трябва да се практикува чрез симулации или настолни упражнения.
- **Координация и споделяне на информация:** Сътрудничеството и споделянето на информация между държавната и местната администрации, както и между държавни агенции и партньори от частния сектор, могат да подобрят колективната кибер устойчивост. Споделянето на информация за заплахи и най-добри практики може да помогне на всички заинтересовани страни да се подготвят и да реагират по-добре на киберзаплахи.
- **Непрекъснато наблюдение и откриване на заплахи:** Внедряването на решения за наблюдение в реално време помага за ранно откриване на киберзаплахи, позволявайки бърз отговор на потенциални атаки. Системите за откриване на проникване, защитните стени и оперативните центрове за сигурност (SOC) играят решаваща роля в това отношение.
- **Сигурни комуникационни канали:** По време на бедствие защитените комуникационни канали стават още по-критични. Осигуряването на криптирани комуникационни инструменти за важните комуникации помага за защита на чувствителната информация от попадане в чужди ръце.
- **Устойчива мрежова архитектура:** Внедряването на гъвкава мрежова архитектура с възможности за резервиране при отказ може да осигури непрекъснатост на предоставянето на услуги, дори ако части от мрежата са компрометирани по време на бедствие.
- **Редовни актуализации на сигурността и управление на корекции:** Поддържането на софтуера и системите актуални с най-новите корекции за сигурност помага за защита срещу известни уязвимости, които кибер нападателите могат да използват.
- **Обществена осведоменост и комуникация:** Обучението на обществеността за потенциални кибер заплахи по време на бедствия и съветването им как да защитят личната си информация и системи също може да допринесе за цялостната киберустойчивост.

Държавните и местните администрации трябва да дават приоритет на устойчивостта на киберсигурността наред с традиционните усилия за готовност при бедствия. Като предприемат проактивни стъпки те могат да подобрят способността си да издържат на кибер заплахи и да осигурят непрекъснатост на критичните услуги по време на бедствия, аварии и катастрофи.

Провеждането на задълбочена оценка на риска помага да се идентифицират потенциални кибер заплахи и уязвимости в инфраструктурата, системите и процесите на организацията. Включва следните стъпки:

1. ***Идентифициране на активи:*** Инвентаризиране на всички критични активи, в т.ч. хардуер, софтуер, данни, мрежи и персонал. Да се разполага с пълноценна информация за всички активи, които се нуждаят от защита, е от решаващо значение за ефективната оценка на риска.

2. ***Идентифициране на заплахи:*** Анализ на потенциални заплахи, които биха могли да повлияят на киберсигурността на организацията. Тези заплахи могат да включват кибератаки, природни бедствия, злополуки, човешки грешки или вътрешни заплахи.

3. ***Оценка на уязвимостите:*** Оценка на слабостите или уязвимостите в цифровата инфраструктура и системите на организацията. Включва потенциални входни точки за кибератаки, остарял софтуер, системи без корекции и несигурни конфигурации.

4. ***Оценка на въздействието:*** Определяне на потенциалното въздействие на идентифицираните заплахи върху дейността, услугите и репутацията на организацията. Оценка на последствията от успешна кибератака или прекъсване, причинено от бедствие.

5. ***Анализ на вероятността:*** Оценка на вероятността за възникване на всяка заплаха, като се вземат предвид исторически данни, разузнаване на заплахите и фактори на околната среда. Това помага да се приоритизират рисковете въз основа на тяхната вероятност за възникване.

6. ***Приоритизиране на риска:*** Класиране на рисковете въз основа на тяхното потенциално въздействие и вероятност. Това помага да се разпределят ресурси и да се фокусира внимание към най-критичните проблеми, свързани с киберсигурността.

7. ***Стратегии за смекчаване:*** Разработка на стратегии за смекчаване на риска за идентифицирани заплахи и уязвимости. Тези стратегии могат да включват технически решения, подобрения на политики, обучение за информираност и планове за архивиране и възстановяване.

8. ***Бюджетиране и разпределяне на ресурси:*** Разпределение на необходимия бюджет и ресурси за ефективно прилагане на набелязаните мерки за намаляване на риска. Това може да включва инвестиране в инструменти за киберсигурност, програми за обучение или наемане на специализиран персонал.

9. ***Мониторинг и преглед:*** Установяване на регулярен процес за преглед, с цел редовна преоценка на рисковете.

10. ***Интегриране с плановете за възстановяване след бедствия и за непрекъсваемост на бизнеса:*** Интегриране на оценката на риска за киберсигурността с цялостните планове за възстановяване.

11. ***Тестване и симулация:*** Провеждане на периодични упражнения и симулации за киберсигурност, за да тестване на ефективността на стратегиите за реакция при инциденти. Тези тестове могат да помогнат за идентифициране на пропуски и области за подобрение.

Резервирането и архивирането са основни компоненти на устойчивостта на киберсигурността и възстановяването след бедствия, като те гарантират, че критичните данни и системи могат да останат налични и функционални дори при кибератаки, бедствия, аварии или други катастрофални събития.

1. ***Резервиране:***

- Резервирането включва създаване на дублирани или алтернативни системи, компоненти или инфраструктура. Ако една система се повреди, резервната система поема дейността, осигурявайки непрекъсната работа.
- Резервните системи могат да бъдат внедрени на различни нива, включително хардуер, мрежи и критични приложения. Например наличието на множество центрове за данни в различни географски местоположения гарантира, че ако един център за данни спре, другият може да поеме работата.

- Резервирането се отнася и до критични роли на персонала, където кръстосаното обучение и резервният персонал гарантират, че основните задачи ще могат да бъдат изпълнени по време на извънредни ситуации или когато ключов персонал не е на разположение.

2. ***Архивиране на данни:***

- Редовното архивиране на данни включва създаване на копия на критични данни и тяхното сигурно съхранение на различни места, за предпочитане извън основния сайт.
- Архивирането може да се извършва с помощта на различни методи, включително пълно архивиране, инкрементално архивиране или диференциално архивиране според нуждите на организацията.
- От съществено значение е да се създаде правилен график за архивиране в зависимост от честотата на актуализации на данните и критичността на информацията. За някои системи може да са необходими копия в реално време.

3. ***Планиране на възстановяване на данни:***

- Наличието на добре дефиниран план за възстановяване на данни е от решаващо значение за ефективното възстановяване на дейността в случай на загуба на данни или повреда на системата. Този план очертава стъпките за възстановяване на данни от архиви и последователността на системите.
- Планът за възстановяване трябва също да определя отговорен персонал за активиране и мониторинг на процеса на възстановяване.

4. ***Тестване и валидиране:***

- Редовното тестване на резервни копия и процедури за възстановяване е от съществено значение, за да се гарантира, че архивите са валидни и че процесите на възстановяване работят според очакванията.
- Провеждането на планирани упражнения за възстановяване помага да се идентифицират всякакви проблеми или пропуски в процеса на възстановяване и позволява проактивно извършване на подобрения.

5. ***Криптиране и сигурно съхранение:***

- Резервните копия трябва да бъдат криптирани, за да се защитят чувствителните данни от неоторизиран достъп или пробиви по време на пренос и съхранение.
- Сигурните места за съхранение, като криптирани облачни услуги или центрове за данни извън обекта, добавят допълнителен слой защита към архивите в случай на физическа повреда или загуба.

6. ***Правила за версии и запазване:***

- Внедряване на политики за управление на версиите и съхранение с цел поддържате множество версии на резервни копия във времето. Това позволява на организациите да възстановяват данни от различни моменти във времето, включително преди възникването на кибер инцидент.

Чрез включването на резервиране и архивиране в своята стратегия за киберсигурност, държавните и местните администрации могат да сведат до минимум времето на престой, загубата на данни и прекъсванията на услугите в случай на бедствия, аварии или кибератаки. Тези мерки са от решаващо значение за поддържането на основни услуги и защитата на чувствителна информация по време на критични ситуации.

Обучението и осведомеността по киберсигурност са жизненоважни аспекти за повишаване на киберустойчивостта на държавните и местните администрации. Човешката грешка и липсата на осведоменост често допринасят за инциденти в киберсигурността. Чрез обучение на персонала относно потенциалните рискове, най-доб-

рите практики и правилните протоколи за сигурност, организациите могат значително да намалят вероятността от успешни кибератаки. Обученията се въвеждат, като:

1. ***Цялостни програми за обучение:*** Разработване и прилагане на цялостни програми за обучение по киберсигурност за служители на всички нива. Тези програми трябва да обхващат различни теми, включително сигурност на паролата, информираност за фишинг, социално инженерство, обработка на данни и процедури за докладване на инциденти.

2. ***Персонализирано обучение за различни роли, които персоналът изпълнява.***

3. ***Редовно и текущо обучение:*** Кибер заплахите и векторите на атаки се развиват бързо, затова обучението по киберсигурност трябва да бъде постоянен процес.

4. ***Симулирани фишинг упражнения:*** Провеждане на симулирани фишинг упражнения, за тестване на способността на служителите да идентифицират и отговарят на фишинг имейли.

5. ***Насърчаване на докладването на инциденти със сигурността:*** поддържане на култура на осведоменост относно киберсигурността, при която служителите се насърчават да докладват незабавно за всякакви подозрителни дейности или инциденти със сигурността. Това насърчава ранното откриване и реагиране на потенциални заплахи.

6. ***Популяризирайте практики за силни пароли:*** Важно е използването на сложни, уникални пароли за всеки акаунт и прилагането на многофакторно удостоверяване (MFA), където е възможно.

7. ***Сигурност на мобилните устройство:*** Обучаване на служителите на най-добрите практики за сигурност на мобилни устройства, тъй като мобилните устройства могат да бъдат уязвими входни точки за киберзаплахи.

8. ***Безопасно използване на интернет и социални медии:*** Обучаване на персонала относно навиците за безопасно сърфиране в интернет, рисковете, свързани с използването на обществен Wi-Fi, и потенциалните опасности от прекалено споделяне на лична информация в социалните медии.

9. ***Обработка на данни и поверителност:*** Обучаване на служителите за правилното боравене с чувствителни лични данни и значението на защитата на информацията.

10. ***Кампании за повишаване на осведомеността:*** Добре информираните и бдителни служители играят решаваща роля в предотвратяването на кибератаки и защитата на критични системи и данни по време на бедствия и други предизвикателни ситуации.

Координацията и споделянето на информация са основни елементи за повишаване на устойчивостта на киберсигурността в държавните и местните администрации по време на бедствия, аварии и катастрофи. Кибер заплахите могат да бъдат сложни и постоянно променящи се, а ефективното сътрудничество между различните заинтересовани страни помага да се изпреварват потенциалните рискове и да се реагира бързо на кибер инциденти. Координацията и споделянето на информация може да се насърчи, чрез:

1. ***Публично-частни партньорства:*** Насърчаване на партньорства между държавната администрация и организации от частния сектор, включително фирми за киберсигурност и оператори на критична инфраструктура.

2. ***Междуведомствено сътрудничество:*** Улесняване на сътрудничеството с различни държавни агенции, отговорни за киберсигурността и реакцията при извънредни ситуации.

3. ***Платформи за споделяне на информация:*** Създаване на защитени платформи за споделяне на информация, където заинтересованите страни могат да споделят информация за киберзаплахи, доклади за инциденти и най-добри практики.

4. ***Споделяне на информация за заплахи:*** Споделяна на информация за киберзаплахи, като индикатори за компрометиране (IOC) и анализ на възникващи заплахи, със съответните партньори.

5. ***Съвместни упражнения:*** Провеждане на съвместни учения и симулации за киберсигурност, включващи множество заинтересовани страни. Тези упражнения помагат за идентифициране на пропуски в координацията и процедурите за реагиране и подобряват цялостната готовност.

6. ***Информационни центрове за киберсигурност:*** Създаване на информационни центрове за киберсигурност на държавно или регионално ниво.

7. ***Форуми между правителството и индустрията:*** Участие във форуми, семинари и конференции на правителството и индустрията, фокусирани върху киберсигурността.

8. ***Съвместни планове за реагиране при инциденти:*** Разработка на съвместни планове за реакция при инциденти, които очертават ролите и отговорностите на различните заинтересовани страни по време на кибер инциденти.

9. ***Междусекторно споделяне на информация:*** Насърчаване на споделянето на информация в различни сектори. Кибер заплахите често са насочени към критични инфраструктурни сектори и споделянето на информация може да засили цялостната кибер устойчивост.

10. ***Сътрудничество между правителството и CERT:*** Сътрудничество с държавни екипи за реагиране при компютърни спешни случаи (CERTs) и подкрепа по време на кибер инциденти.

11. ***Регулаторна подкрепа:*** Прилагане на обща регулаторна, която насърчава споделянето на информация между заинтересованите страни, като същевременно гарантира поверителността и сигурността на данните.

Осъществяването на непрекъснат мониторинг и откриването на заплахи включва активно наблюдение на цифрови системи и мрежи за идентифициране и реагиране на потенциални кибер заплахи и атаки в реално време. Чрез ранно откриване на заплахи организациите могат да предприемат бързи действия за смекчаване на тяхното въздействие и защита на критични активи. Това може да бъде осъществено чрез:

1. Система за управление на информация и събития, свързани със сигурността (SIEM): Внедряване на SIEM за събиране корелиране и анализ на регистрирани данни от различни източници, включително сървъри, защитни стени, рутери и приложения. SIEM инструментите осигуряват централизиран поглед върху състоянието на сигурността на организацията и позволяват откриването на подозрителни дейности и аномалии.

2. Системи за откриване на проникване (IDS) и системи за предотвратяване на проникване (IPS): Използвайте IDS и IPS, за да наблюдение на мрежовия трафик за признаци на неоторизиран достъп, зловреден софтуер или подозрително поведение. IDS открива потенциални заплахи, докато IPS може да предприеме автоматизирани действия за блокиране или смекчаване на заплахи в реално време.

3. Анализ на поведението: Въвеждане на поведенчески анализи, с цел установяване на базова линия на нормално потребителско и системно поведение. Това помага за откриването на аномалии, които могат да показват потенциални вътрешни заплахи или кибератаки.

4. ***Информиране от специализирани източници за активни и нови заплахи.***
5. ***Сканиране за уязвимости и незабавно прилагане на корекции за сигурност.***
6. ***Откриване и реакция в крайните точки (EDR):*** Използване на EDR решения в работни станции и лаптопи, с цел мониторинг и реакция на подозрителни дейности на ниво крайна точка. Това подобрява видимостта и контрола върху потенциалните заплахи.
7. ***Откриване на аномалии и машинно обучение:*** Използване на техники за откриване на аномалии и машинно обучение, за идентифициране на модели, присъщи за киберзаплахи, които може да бъдат предизвикателство за откриване с традиционните подходи, основаващи се на правила.
8. ***Анализ на мрежовия трафик:*** Анализ на моделите на мрежов трафик с цел откриване на всякакви необичайни или неоторизирани дейности. Разширеният анализ може да помогне за идентифициране на индикатори за компрометиране (IOC) и потенциални опити за ексфилтрация на данни.
9. ***Анализ на потребителското поведение (UBA):*** Използва се за проследяване на потребителски дейности и откриване на необичайно поведение, което може да показва вътрешни заплахи или компрометирани акаунти.
10. ***Непрекъснато търсене на заплахи:*** Търсене на проактивни признаци на неоткрити заплахи в мрежата. Този подход помага за откриване и неутрализиране на заплахи, преди да причинят значителна вреда.
11. ***Автоматизирана реакция при инциденти:*** Внедряване на автоматизирани работни процеси за бързо реагиране на идентифицирани заплахи, чрез автоматизирани незабавни отговори.
12. ***Оперативни центрове за сигурност (SOC):*** Създаване на SOC или използване на управлявани услуги за сигурност, за осигуряване на 24/7 мониторинг, откриване на заплахи и възможности за реакция при инциденти.

Непрекъснатият мониторинг за заплахи допълват другите мерки за киберсигурност и допринасят за способността на организацията да открива и реагира ефективно на киберинциденти.

Сигурните комуникационни канали са от съществено значение за защита на чувствителна информация и гарантиране на поверителност, цялост и автентичност по време на предаване на данни. Някои ключови елементи и технологии са:

1. ***Криптиране:*** Криптирането от край до край гарантира, че данните остават защитени през целия им път от подателя до получателя.
2. ***Виртуални частни мрежи (VPN):*** VPN създават сигурни, криптирани тунели през обществени мрежи, като интернет, позволявайки на отдалечени потребители и офиси да имат защитен достъп до вътрешните ресурси.
3. ***Сигурност на транспортния слой (SSL/TLS)*:** SSL/TLS протоколите установяват сигурни връзки между уеб сървъри и браузъри, като гарантират, че данните, обменяни през уебсайтове са защитени.
4. ***Защитени протоколи за прехвърляне на файлове:*** Защитените протоколи за прехвърляне на файлове като SFTP (SSH протокол за прехвърляне на файлове) и SCP (протокол за защитено копиране) позволяват защитен обмен на файлове между системите.
5. ***Сигурна имейл комуникация:*** Криптиране на имейл и използване на цифрови подписи за защитите на комуникацията по имейл. Технологии, като S/MIME (Secure/Multipurpose Internet Mail Extensions) и PGP (Pretty Good Privacy) осигуряват криптиране на имейл от край до край.

6. ***Инфраструктура с публичен ключ (PKI):*** PKI е рамка, която използва цифрови сертификати и криптографски ключове, за да гарантира автентичността на потребителите и сигурна комуникация.

7. ***Сигурна гласова и видео комуникация:*** За гласова и видео комуникация могат да се използват технологии, като протокол за глас през интернет (VoIP) със защита на транспортния слой (TLS) или защитен транспортен протокол в реално време (SRTP) за криптиране на комуникацията.

8. ***Многофакторно удостоверяване (MFA):*** Внедряването на MFA добавя допълнително ниво на сигурност към комуникационните канали, като изисква множество форми на удостоверяване за проверка на самоличността на потребителя.

9. ***Защитни стени и системи за откриване/предотвратяване на проникване (IDS/IPS):*** Тези мерки за сигурност предпазват комуникационните канали, като наблюдават и контролират входящия и изходящия трафик.

10. ***Провеждане на регулярни одити и оценки.***

Внедряването на сигурни комуникационни канали е от съществено значение за държавните и местните администрации за защита на чувствителна информация, предотвратяване на пробиви на данни и поддържане на доверието на гражданите. Чрез възприемане на стабилни методи за криптиране и използване на различни защитени комуникационни технологии, организациите могат да намалят риска от неоторизиран достъп и прихващане на данни, особено по време на бедствия или извънредни ситуации, когато защитената комуникация става още по-критична.

Устойчивата мрежова архитектура е подход на проектиране, който гарантира наличността, надеждността и непрекъснатостта на мрежовите услуги дори при повреди, кибератаки, бедствия и други предизвикателни ситуации. За държавните и местните администрации, устойчивата мрежова архитектура е от решаващо значение за поддържането на критични услуги и комуникация по време на извънредни ситуации. Ето някои ключови принципи и компоненти на устойчивата мрежова архитектура:

1. ***Резервиране и висока наличност:*** Резервиране на различни нива, като мрежови връзки, комутатори, рутери и сървъри.

2. ***Дизайн на разпределена мрежа:*** Избягване на единични точки на повреда, чрез разпределение на мрежовите ресурси в различни географски местоположения.

3. ***Балансиране на натоварването:*** Прилагане на техники за равномерно разпределяне на мрежовия трафик между множество сървъри или маршрути.

4. ***Много маршрутна свързаност за приложения или центрове за данни.*** Подобрява устойчивостта.

5. ***Софтуерно дефинирана мрежа (SDN):*** SDN позволява централизирано управление на мрежата и динамично разпределение на ресурси в реално време.

6. ***Приоритизиране на качеството на услугата (QoS):*** Използване на QoS, за приоритизиране на критичен мрежов трафик.

7. ***Сегментиране на мрежата:*** Сегментиране на мрежата в отделни зони или виртуални LAN (VLAN), за ограничаване на въздействието на потенциални пробиви.

8. ***Използване на облачно базирано резервиране.*** Дава възможност за продължаване на работата при проблеми с локалната инфраструктура.

Редовните актуализации на сигурността и управлението на корекциите са решаващи компоненти за поддържане на сигурна и устойчива ИТ инфраструктура. Като приоритизират актуализации на сигурността и управлението на корекциите, държавните и местните администрации могат значително да намалят излагането си на киберзаплахи, да подобрят цялостната устойчивост на киберсигурността и да защитят критичната инфраструктура и чувствителните данни от експлоатация.