https://doi.org/10.70265/GQVY3715

ПРАВИЛА И ЕЛЕМЕНТИ ЗА СИГУРНОСТ НА ДАННИТЕ

Теодора Личева

DATA SECURITY RULES AND ELEMENTS

Teodora Licheva

Резюме: *Данните са ключът към успеха на всяка структура. За да могат да гарантират сигурност, неманипулираност и достоверност на информацията, както в облака, така и в реална среда е необходимо да се въведат нови стратегии, елементи и правила. Наложително е организациите да отговорят на изискванията на съвременната бизнес среда и да са една крачка пред конкурентните и злонамерени действия.*

Ключови думи: *сигурност, данни, правила*

Summary: *Data is the key to the success of any organization. In order to ensure the security, integrity and authenticity of information, both in the cloud and in real environments, it is necessary to introduce new strategies, elements and rules. It is imperative for organizations to meet the requirements of the modern business environment and stay one step ahead of competitive and malicious actions.*

Keywords: *security, data, rules*

УВОД

Данните са най-ценната принадлежност на една организация, независимо дали става въпрос за държавна институция или фирмена структура. Дигитализацията и свързхсвързаността променят методите за събиране, обработване, записване, трансфер, използване и архивирането им (Европейска комисия, 2020). За да бъдат данните достоверни, неманипулирани и защитени трябва да се предприемат действия, който да ги предпазят от киберпрестъпления – както в реална среда, така и в облака. Настоящото изследване предлага етапите за създаване на ясни правила и елементи при събирането, обработването и използването на данни, които са от ключово значение за просперитета на организацията.

1. ТЕХНИКИ И ПРАВИЛА ЗА ГАРАНТИРАНЕ СИГУРНОСТ И ДОСТОВЕРНОСТ НА ДАННИТЕ

За да може една организация да защити правилно данните си, тя трябва да знае какъв вид данни има. От ключово значение да се направи анализ на генерираните и събрани данни и да определи вида им, за да се улесни управлението, съхранението и защита им. С тези действия и процеси се създава класификационна система, в съответствие със законовите и нормативни разпоредби и се изгражда стратегията на сигурност на данните във всяка организация.

Фигура 1. Технологии и процеси за гарантиране сигурността на данните

1.1 Защитна стена

Защитните стени действат като контролна точка за сигурност и представлява защитна преграда между вътрешните и външните мрежи. Всъщност тази функция е първата защита на личната информация. Нейната роля е да контролира, наблюдава и филтрира входящия и

изходящ мрежови трафик, като прилага заложени в програмата правила и норми за сигурност.

Правилата за сигурност ще допуснат или блокират информационния поток. Характеристики на защитните стени са:

- контрол на трафика;
- контрол на достъпа;
- разделяне на подмрежи;
- откриване и блокиране на злонамерени мрежови дейности в реално време;
- виртуална частна мрежа[1];
- съхраняват логове на мрежовия трафик, за наблюдение и откриване на потенциални заплахи.

1.2 Криптиране на информацията

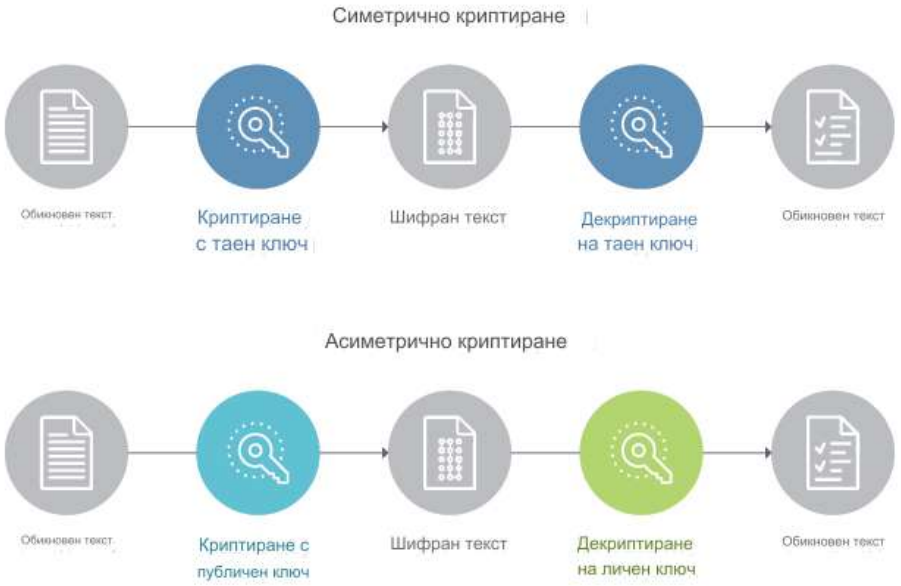
Криптиране или шифроване е процес, при който предаваните данни могат да бъдат интерпретирани и разчетени само от получателя. Криптираният текст от четим се преобразува в неподлежащ на разчитане вид, с помощта на алгоритъм за шифроване или код. Данните са безполезни, ако изтекат в мрежата или бъдат откраднати, защото не могат да бъдат прочетени и декриптирани, ако не е наличен свързан ключ за декриптиране. Само организация или служител, с правилен ключ може да прочете текста.

Често се срещани следните основни разновидности:

1. Симетрично криптиране. При него се използва един таен ключ, както за криптиране, така и за декриптиране. Този вид шифроване е бърз и лесен за настройване, но изисква механизъм за сигурно споделяне на тайния ключ в мрежата на интернет.

2. Асиметрично криптиране. Този вид криптиране използва два взаимосвързани ключа: публичен ключ – за криптиране и частен ключ – за декриптиране на данните. При този вид кодиране не се разменят ключовете, което повишава сигурността, а цифровите подписи позволяват да се удостовери подателя. Недостатък може да е забавяне на процеса, ако се загуби ключа и данните не могат да се декриптират.

[1] Виртуалната частна мрежа (*англ*. Virtual Private Network) е механизъм за защитна връзка между изчислителното устройство и компютърната мрежа/и.



Фигура 2. Разлика между симетрично и асиметрично криптиране (Източник: Cobb, 2022a)

3. Криптографско хеширане. Това кодиране има различна функция. Хешироването е процес, при който данните се преобразуват в поредица от фиксирана дължина от буквено-цифрови знаци. Тази дейност е математически алгоритъм. Хеш функцията е пръстовият отпечатък на данните, като при технологията на блокова верига – блокчейн.

Според вида на информацията се избира алгоритъм за криптиране. Личните и чувствителни данни трябва да са най-добре криптирани (Личева, 2023, с. 94).

1.3 Контрол на достъп

Един от най-ефикасните методи за защита на информацията е да има контролиран достъп до нея. Структурата трябва така да организира дейността си, че само упълномощени служители да имат право да използват, редактират и изтриват данните. Контролираният достъп се осъществява от две дейности:

- първата стъпка е самият потребител да удостовери, че е този за който се представя;
- следващото действие е служителят да удостовери, че има достъп до исканото ниво на информация.

В последно време все по-популярна и с широко приложение е стратегия за контрол на достъпа с нулево доверие. Тази рамка е подход за киберсигурност, която отказва достъп до цифрови ресурси на организацията по подразбиране и предоставя на удостоверени

потребители и устройства, персонализиран, отделен достъп и само и единствено до приложения, данни и услуги, които са им необходими за да извършват дейностите си (Irei, n.d. a).

1.4 Маскиране на данни

Маскирането на данни е процес, при който реалните данни се маскират с произволни знаци. По този начин чувствителната информация не може да бъде видяна, от лица, които нямат разрешение да я видят.

За да се извърши процеса по маскиране на данни, първо трябва да се създаде копие на базата данни, която напълно да отговаря на оригиналната. Маскирането на данни защитава чувствителната информация в реално време.

Методите за маскиране са следните (Cobb, 2022b):

1. Замаскирване – използва се при промяна само на част от стойностите на данните.

2. Разбъркване – използват се буквено-цифрови знаци, за да се скрие оригиналното текстово съобщение.

3. Заместване – заменят се оригинални данни с други стойности. Често в справочни таблици се предоставят заместващи стойности на оригиналната чувствителна информация. Заместващата техника е по-трудно приложима от разбъркващата.

4. Разместване – прилага се при разместване на стойностите в колона. Може да се използва само за разместване на имена, като резултатите изглеждат правилни, но всъщност не се разкрива лична информация.

5. Вариране – прилага се, когато се маскира финансова или трансакционна стойност към информация за датата. Алгоритъмът променя всяко число или данни в колоната с произволен процент от истинската стойност. Ако се използва един и същ процент за данните се счита разумно прикриване.

6. Нулиране – използва се, когато се заменят реални данни в колона със стойност нула. Нулираната колона не може да има повторно използване или да участва в анализ на данните;

7. Промяна на датите – приложението може да увеличи или намали данните за определен период от време.

В зависимост от необходимостта и начина за маскиране се разграничават следните разновидности:

Фигура 3. Видове маскиране на данни

Процесът по маскиране на данни е с широко приложение, особено когато се тества софтуер, използва за обучение на потребители и за анализ на данни. Но този процес не се използва за самите чувствителни данни.

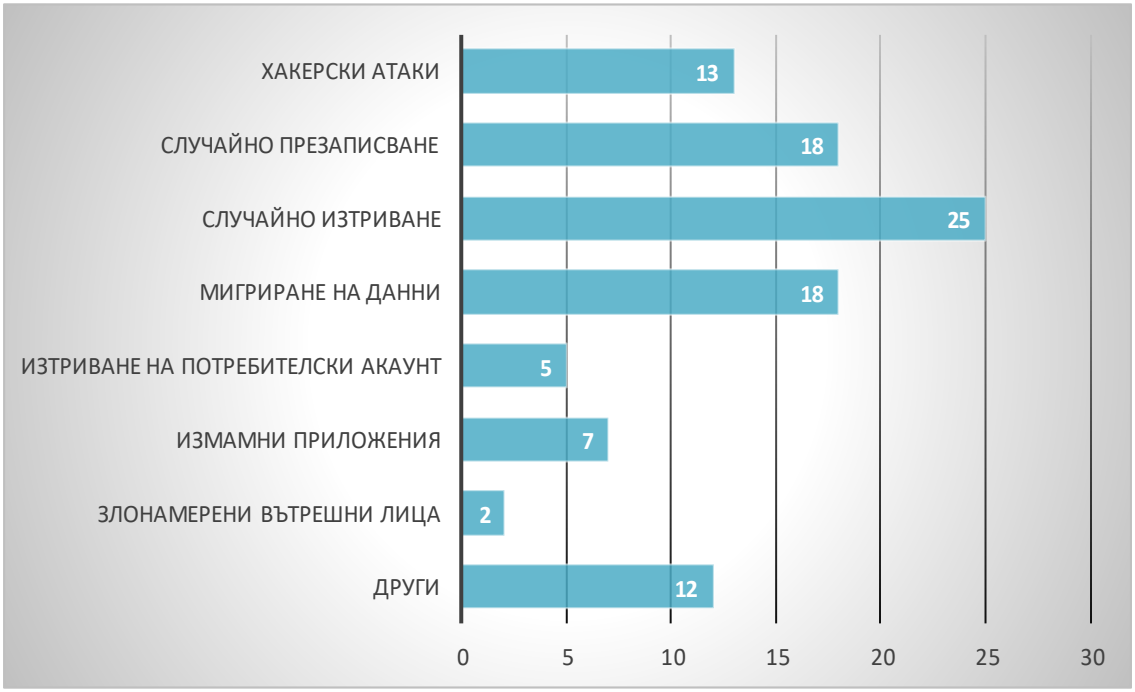
Както вече бе посочено криптирането е най-сигурният начин за съхранение и трансфер на чувствителните данни, но кодираните данни са трудни за анализ, докато маскираната информация е неразпознаваема, но все пак може да се използва. Шифрованите данни могат да бъдат дешифрирани и да възстановят оригиналния си вид с правилния ключ, докато за маскираните данни няма алгоритъм за възстановяване на първоначалните стойности.

1.5 Предпазване от загуби на данни

С различни софтуерни инструменти и практики може да се предотврати изтичането на данни и да се ограничи достъпът до чувствителна информация. Създаването на стратегия, която да предпазва от загуба на данни ще гарантира, че данните ще останат зад мрежовата защита.

Внедряването на софтуер за защита ще извършва мониторинг, ще открива и блокира данните, така че да не може да излязат извън

защитната стена. Най-често дейностите, които предотвратяват изтичане на данни са с блокиращо действие, което дори може да включва невъзможност за запис на флаш памет, за да няма неоторизирано копиране на данните.



Фигура 4. Причини за загуба на данни

Загубата на данни може да доведе до административни и наказателни санкции, да повлияе върху бизнес процесите и дори да предизвика фалит на организацията. Доверието на обществото и на клиентите ще е разклатено и ще е трудно да се възстанови благоприятния бизнес климат.

1.6 Хардуерна сигурност

Сферата на информационно-комуникационните технологии се развива непрекъснато. И това налага да се търси стабилна защита срещу кибератаки и въвеждането на политика да борба с киберпрестъпленията да е задължителна част от стратегията за сигурност на всяка организация.

Хардуерната сигурност представлява защита от външни физически устройства, а не от софтуер, инсталиран в компютърната система. Обикновено това са хардуерни защитни стени и прокси сървъри. Хардуерната сигурност гарантира по-голяма сигурност от софтуерната и често включва допълнителен слой за сигурност.

Защитните стени не са достатъчно средство, за да гарантират цялост и конфиденциалност на базите данни, особено на

наследствените мрежи, които преминават към съвременни цифрови системи.

Хардуерните елементи за сигурност са насочени към откриване на нерегламентирано проникване, автоматично и ръчно изолиране на мрежата, както и устройства за защита на крайните точки. Тези елементи са допълнителен слой за хардуерна защита и гарантират сигурност на мрежата в реално време.

1.7 Системи за архивиране и съхранение

Системите за архивиране и съхранение създават копия на бази данни и на файлове, които могат да се използват многократно. В случай, че оригиналните данни бъдат източени, повредени или манипулирани, архивирането гарантира тяхното възстановяване в първично състояние.

Архивирането на данни ги предпазва от човешки грешки, кибератаки, хардуерни повреди и природни бедствия и катаклизми. Архивирането е успешно, ако може да възстанови бързо и точно личните и чувствителни данни за организацията.

В практиката на организациите се е наложила стратегията 3-2-1, която определя да има три копия на данните. Тези копия трябва да са съхранени на два различни носители, като е задължително едно копие да е извън базите данни на организацията. Често това е облачното архивиране (Личева, 2022, с. 58), особено при отдалечено работно място и дистанционна работа, защото киберсигурността не е толкова силна в домашни условия и на личните устройства.

Фигура 5. Принцип на стратегията 3-2-1 за архивиране и съхранение на данни

Друга характеристика, на която трябва да се обърне внимание е устойчивостта на системата, като под устойчивост на системата се разбира адаптиране и възстановяване на системата след кибератака или друго зловредно действие.

1.8 Изтриване на данни

Изтриването на данни гарантира, че изтритите данни не могат да се възстановят, дори и при достъп на неоторизирани потребители.

Техниката за изтриване на данни включва цялостно презаписване на данните, но по начин, че те да не могат да бъдат възстановени. Много често данните се превръщат в нечетливи, след като бъдат изтрити.

Тази практика е основна в областта на сигурността и поверителността на данните. С процесът данните се унищожават от устройствата за съхранение – твърди дискове, устройства и други цифрови носители чрез софтуер или друг метод. Този процес е напълно невъзстановим, но устройството може да се използва многократно.

Четири са основните техники за извършване на процеса изтриване на данни:

1. Презаписване. Носителят на данни се презаписва с нови данни.

2. Кодиране. Техниката предпазва данните от нерегламентиран достъп.

3. Повреда на устройството. Често чрез повреда на магнитното поле на диск или друго преносимо устройство данните се изтриват. При тази техника трябва да се отбележи, че диска мога да се преформатира и да се възстановят фабричните настройки.

4. Физическо унищожаване на данните. С този метод се унищожава напълно носителят на данни. Дори малка част от диска съдържа данни и затова трябва се ликвидира цялото устройство или диск.

2. ДЕЙНОСТИ ПРИ КИБЕРАТАКИ

Пет са основните дейности за реагиране при кибератака (Kirvan, 2023):

1. Идентифициране на заплаха. В тази дейност са включени редица поддейности като: оценка на риска, заплаха и уязвимост. Целта е да се определят потенциалните заплахи за организацията, както и размера на атаката.

2. Защита. Тази дейност обхваща дейностите като защитни стени, системи за откриване и предотвратяване на проникване, както софтуер за анализ на сигурността.

3. Откриване. Тази мярка обхваща системи за сигурност, благодарение на които да се открие потенциалния възможен злонамерен код.

4. Отговор на системите за сигурност. Дейността обхваща анализи и последващи дейности, които да изолират зловредната атака и да я неутрализират, за да предотврати по-нататъшни щети по системата.

5. Възстановяване. Тази стъпка обхваща всички дейности, които да възстановят повредените системи и данни, за да подпомогна организацията да възобнови дейността си по най-бързия начин.

При правилно и целесъобразно извършване на гореизложените дейности, организацията ще може бързо да се върне в нормалния си работен режим и да има по-малко загуби при извършване на кибератака или изтичане на данни.

В последните години става все по популярен термина киберхигиена (Irei, n.d. b). По своята същност това понятие включва всички дейности и практики, които запазват чувствителните данни защитени и засилва способността на организацията да се възстанови, ако стане жертва на успешна кибератака. Концепцията на киберхигиената е подобна да човешката, лична хигиена. Организацията трябва да поддържа здравето на системите си, така че да предотврати пробиви и теч на лични данни и инциденти със сигурността, като следва основни принципи.

Поддържайки киберхигиена организацията подобрява мерките на сигурност, като минимализира риска от атаки, манипулиране и загуба на данни.

Киберсигурността предпазва от заплахи, докато киберустойчивостта подобрява състоянието на системите на организацията и подпомага тяхното възстановяване и възобновяване на нормалните работни процеси, след пробив в сигурността. В основата на двете понятия е киберхигиената.

3. ПРЕДИЗВИКАТЕЛСТВА ПРЕД СИГУРНОСТТА НА ДАННИТЕ

Колкото по-голям обем са данните, толкова по-трудно е те да бъдат защитени. Съвременните организации са изправени пред редица предизвикателства, за да ги опазят.

Част от тях са:

1. Вътрешни заплахи. Те са най-голямата заплаха за сигурността на данните. Тази категория опасност идва от служители, които имат достъп до физически и/или цифрови актива на организацията, т.е. от вътрешни лица. Това може да са настоящи служители, бивши служители, изпълнители, бизнес партньори и доставчици, т.е. всички, които са имали разрешен достъп до данните на организацията. С вътрешната атака може да има манипулиране на данни, измама, саботаж на мерките за сигурност, кражба на интелектуална собственост или търговска тайна. Вътрешната заплаха може да се раздели на три подраздела (Froehlich, Hanna, & Posey, 2022):

- Настоящи служители – имат възможност да откраднат чувствителни данни и да се облагодетелстват лично;

- Бивши служители – умишлено запазват достъп до системите на организацията с цел да саботират мерките за сигурност или за да навредят с кражба на чувствителни данни, за лична изгода или отмъщение.

- Неволни действия на служители – по невнимание или липса на осведоменост не спазват политиката на сигурност на организацията. При използване на служебни системи и данни мога да спомогнат за фишинг атаки, зловреден софтуер и др. опасности за данните.

2. Грешни конфигурации на компонентите. Технически неправилните компоненти също са голяма заплаха и често водят до изтичане на данни и разкриване на чувствителна информация;

3. Риск от трета страна. Общоприето е, че организацията е толкова сигурна, колкото е сигурен всеки един от партньорите ѝ, независимо дали е доставчик, клиент или изпълнител по веригата.

Всяка организация, независимо дали е в частния или държавния сектор, трябва има изградени правила за сигурност на информацията. Това може да са насоки, вътрешнофирмени правила, регламенти или стратегия, но важното е да се създават и опишат инструментите, технологиите и техниките за сигурност.

Фигура 6. Акценти при изготвяне на правила за сигурност на данните

ЗАКЛЮЧЕНИЕ

Изготвяне на стратегия и стратегически план за изпълнение й, по отношение защита на данните на организацията, ще допринесе за ефективното им използване, актуализиране на мерките за сигурност и управлението на риска.

Внедряването на системи за непрекъснат мониторинг и наблюдение ще ограничи неправилното им използване, достъп и злонамерени действия в реално време и в облака.

Инвестициите в изграждането на стратегии и правила за сигурността на данните трябва да са приоритет, за да могат организациите да са поне една крачка пред извършителите на злонамерени действия и заплахи.

ЛИТЕРАТУРА:

Европейска комисия. (2020). *Европейска стратегия за данните*. Служба за публикации на Европейския съюз. https://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:52020DC0066

Личева, Т. (2022). *Цифрови трансформации в архивното дело*. Научно-технически съюз по машиностроене „Индустрия 4.0“.

Личева, Т. (2023). *Модерна сигурност в управлението*. Научно-технически съюз по машиностроене „Индуктрия-4.0.

Cobb, M. (2022a, July 22). *Symmetric vs. asymmetric encryption: What's the difference?* TechTarget. https://www.techtarget.com/searchsecurity/answer/What-are-the-differences-between-symmetric-and-asymmetric-encryption-algorithms

Cobb, M. (2022b, August 11). data masking. In Shea, Sh. (Ed.), *What is data security? The ultimate guide*. TechTarget. https://www.techtarget.com/searchsecurity/definition/data-masking

Froehlich, A., Hanna, K. T., & Posey, B. (2022). insider threat. In Shea, Sh. (Ed.), *What is data security? The ultimate guide*. TechTarget https://www.techtarget.com/searchsecurity/definition/insider-threat

Irei, A. (Ed.). (n.d. a). *What is the zero-trust security model?* TechTarget. https://www.techtarget.com/searchsecurity/definition/zero-trust-model-zero-trust-network

Irei, A. (n.d. b). *What is cyber hygiene and why is it important?* TechTarget. https://www.techtarget.com/searchsecurity/definition/cyber-hygiene

Kirvan, P. (2023, October 17). *How to conduct a cyber-resilience assessment*. TechTarget. https://www.techtarget.com/searchsecurity/tip/How-to-conduct-a-cyber-resilience-assessment