Технически Университет – София

Факултет Приложна Математика и Информатика

Катедра Информатика

КУРСОВА РАБОТА

Тема: Cyber security frameworks in healthcare

Имена на студента: Станислав Бисеров Стоянов

Факултетен номер, група: 471218066, 76 група

Съдържание:

1. Увод

Киберсигурността или ИТ сигурността използват работна рамка (framework), която се фокусира върху защитата на компютрите, програмите, данните и мрежи от неоторизиран или непредвиден достъп. Правителствените агенции, корпорации, военните, болниците, финансовите институции и много други организации често са склонни да събират, съхраняват и обработват лична поверителна информация на своите системи и мрежи. С нарастващата сложност и обем на атаките в киберпространството, има нужда от засилено внимание за защита на чувствителната информация, както и за защита на националното здравеопазване и сигурност. Комуникацията по интернет и компютрите като цяло представляват изключително сложни инженерни изобретения, които от своя страна имат много неразгадани предизвикателства. Предизвикателства, които варират от защитата на целостта на данните (protection integrity) до конфиденциалността по отношение на предадени данни и информация. Работните рамки по киберсигурност (cyber security frameworks) в здравеопазването имат ключова роля за опазване на сензитивните биологични данни на потребителите.

2. Какво е cybersecurity framework (CSF)?

Рамките за киберсигурност (cybersecurity frameworks – CSF) са пътните карти (roadmaps) при ИТ системите за сигурност. CSF е ръководство (guide), базирано на вече съществуващи насоки и практики. Основната роля на CSF е да подпомогне организациите да намалят проблемите със сигурността и да се справят с процесите на управление (management processes) - например дава насоки на администраторите как да управляват пациентските лични данни. Работните рамки в здравеопазването като всяка една технология се актуализират чрез получаване на адекватна информация от ползвателите им. Все още, тези фреймуърци не са точни предписания (prescriptions). Те могат единствено да предложат само общи методи за справяне с кибер заплахите. Например, когато една болница изгражда EHR система за дигитализиране на взаимотношенията между пациент и лекар и се фокусира върху елиминирането на проблемите със сигурността и изтичането на някакви сензитивни данни, тези фреймуърци предоставят начини за справяне с евентуалните бъдещи проблеми в системата. Важно е да се спомене, че фреймуърците не са единственият начин за защита на данните. Те са доказан подход за разработване на политики и процедури, необходими за гарантиране на поветирелността, целостта и наличието на информационни системи и данни. Организациите за здравеопазване могат да избират от редица фреймуърци, които са широко използвани и редовно поддържани.

3. Какви са основните цели на CSF?

- Описва сигурността на ситуацията (security situation)
- Описва целта на сигурността (security posture)

- Непрекъснато подобрение
- Премахване на комуникационните рискове (communication risks)

4. От какво се състои един CSF?

- *Ядро* - позволява комуникацията между киберсигурност рисковете (cybersecurity risks) в една организация;
- *Нива на изпълнение (implementation tiers)* - помагат да се намери правилното ниво на задълбоченост (thoroughness) за дадена програма за сигурност;
- *Профили (profiles)* – привеждат в съответствие индустриалните стандарти и най-добри практики, подпомагат приоритизирането и измерването (measurement);

5. С какво допринасят за здравеопазването?

Да си признаем, че здравеопазването е индустрията, в която вътрешните заплахи за сигурността са по-опасни от външните. Според доклада на Verizon, вътрешните заплахи (threats) са по-чести в една здравна организация – 59% в сравнение с 41% за външните. Причини? Различни грешки, злоупотреба с привилегии или софтуерни проблеми са едни от основните причини за тези заплахи. Служителите често злоупотребяват с достъпа си до вътрешната информация. Освен това, в 6% от случаите на вътрешно изнасяне на конфиденциална информация, целта е била просто забавление, което изобщо не е смешно като цяло. Нищо учудващо няма във факта, че здравеопазването осигурява необходимостта от защита, поверителност и сигурност на личните данни на обществото чрез използването на специални рамки за киберсигурност (cybersecurity frameworks).

6. С какво ни помагат CSF?

1. Рамките помагат за идентифицирането и откриването на заплахи, свързани със сигурността и възстановяването от тези последствия
2. Те гарантират сигурност със своите компоненти – ядро, ниво на изпълнение и профили
3. Позволяват на заинтересованите страни (stakeholders) да разбират и управляват киберсигурността заедно като екип
4. Помагат развитието на бизнеса (aligning business) и технологичните политики

7. Топ 5 CSF в здравеопазването – извадката се базира на HIMSS Cybersecurity Survey

Framework #1. NIST

Най-популярният фреймуърк за сигурност в здравеопазването е NIST, като 57.9% от анкетираните в проучване проведено през 2018г. (HIMSS Cybersecurity Survey) съобщават, че го използват в своите организации. NIST е национален институт за стандарти и технологии, американска агенция, която разработва много технически стандарти и насоки (guidelines), включително за информационна сигурност. Тази агенция е една от многото в САЩ под контрола на Министерството на търговията (U.S Department of Commerce).

Framework #2. HITRUST

Малко повече от една четвърт от анкетираните (26.4%) казват, че тяхната организация следва рамката за сигурност (security framework), поддържана от Health Information Trust Alliance (HITRUST). HITRUST Alliance е частна организация, ръководена от представители на някои от най-големите имена в здравеопазването като Anthem, Humana, UnitedHealth и Walgreens.

Framework #3. CIS Critical Security Controls

Малко по-малко от една четвърт (24.7%) от анкетираните заявяват, че използват Critical Security Controls. Center for Internet Security (CIS) е нестопанска организация, която поддържа 20 Critical Security Controls (CSC, познато още като SANS 20). CSC е списък на различни практики за киберсигурност, предназначени да спрат най-често срещаните кибератаки.

Framework #4. ISO

ISO е Международна организация за стандартизация (International Organization for Standardization), неправителствена организация, която публика стандарти за улесняване на световната търговия. Членството се състои от представителни различни агенции в повече от 160 страни. Заедно с Международната електротехническа комисия International Electrotechnical Commission (IEC), ISO налага серия от стандарти за създаване и поддръжка на информационната система за управление и сигурност (information security management system), известна като ISO/IEC 27000 или просто ISO. Сред анкетираните, 18.5% използват този фреймуърк.

Framework #5. COBIT

COBIT означава Control Objectives for Information and Related Technologies, рамка за сигурност създадена от ISACA (позната още като Асоциация за одит и контрол на информационните системи – Information Systems Audit and Control Association). Около 7.3% от анкетираните заявяват, че използват тази рамка за сигурност.

8. Как да имплементираме CSF?

Рамките за сигурност вършат чудесна работа, но как да започнем да ги използваме? Повечето болници следват следните шест стъпки на интегриране, така че ние ще прегледаме детайлно всяка една от тях.

Стъпка #1: Очертаване на приоритетите

Всичко започва с определяне на целите и приоритетите на здравната организация. Също така анализът на текущите заплахи и въздействия е съществено важен. Прави се с цел вземане на най-добрите решения относно проблемите със сигурността и подбор на правилните инструменти, които да предоставят адекватни решения за проблема. Следователно, преди да преминем към интегрирането, болницата или клиниката трябва да разберат къде и как точно искат да използват дадената рамка за киберсигурност (cybersecurity framework).

Стъпка #2: Дефиниране на подходи за управление на риска

Първо, организацията трябва да очертае какви инструменти, технологии и чувствителни данни има и използва. Тя трябва да изчисли цялостния подход за риск и да определи своите слаби страни в системата. След това, компанията избира подходящия регулатор (regulatory) – стандарти за сигурност, средства, методи и т.н.

Стъпка #3: Оценяване на рисковете

Тази стъпка е свързана с оценката нивото на риска в настоящата информационна система. Организацията анализира колко сериозни нарушения на сигурността биха могли да се появят и от какво могат да бъдат предизвикани. Също така, компанията взима предвид настоящите уязвимости и заплахи с цел да разбере по-добре какви могат да бъдат бъдещите проблеми със сигурността.

Стъпка #4: Създаване на профил за управление на риска

Както споменах в началото, рамките за сигурност не са идеалното решение. Най-ефективните имплементации са съобразени с конкретния бизнес. Следователно следващата стъпка е адаптиране на рамката според нуждите на организацията. Болниците правят задълбочена оценка на риска и определят настоящето си състояние. По-добре е тези рискове да се оценят от функционалните области (functional areas) и от цялата организация, независимо. И ако се открият рискове, те незабавно трябва да бъдат документирани.

Стъпка #5: Изготвяне на план за действие

Когато организацията е оценила рисковете и техните последствия, тя може да започне да сравнява реалните резултати с желаните. Например, създаването на гореща карта (heat map), която да покаже резултатите и да маркира областите, на които трябва да се обърне сериозно внимание. След това идва "brainstorming" – тя трябва да намери с какво точно да запълни празнината между текущия и целевия резултат.

Стъпка #6: Изпълнение на плана за действие

Към този момент, компанията трябва да има:

- ясна картина на проблемите на киберсигурността, с които може да се сблъска
- налични "отбранителни" средства
- конкретни цели
- анализ на пропуските
- списък с действията за предприемане

Ако всички тези стъпки са на лице, тогава може да се започне внедряването на фреймуърка, който са избрали. Но това не завършва само с приемането на план за действие. Здравните институции трябва да организират и наблюдават различни показатели, за да бъдат сигурни, че CSF работи така както се очаква. Това е непрекъснат процес, който цели да доведе до получаване на максимална печалба и по-нататъшно персонализиране на приетия фреймуърк. Което в крайна сметка би трябвало да отговаря напълно на нуждите на компанията.

9. Заключение

Като един от основните въпроси по темата, свързана с глобализацията и защитата на потребителските данни, някои от подходящите фреймуърци обсъдени по-горе, трябва да бъдат взети под внимане. Това е важно, тъй като киберпрестъпленията и киберзаплахите доведоха до огромни загуби в различни частни и правителствени организации. От друга страна, тези рамки могат да нарушат системите за сигурност и управление на дадена държава поради анализа на чувствителни (строго секретни) данни и информация. Крайното решение следователно трябва да включва формирането на подходящи закони за управление на здравеопазването и ясни регулации какво може да се прави с потребителските биологични данни.

10. Използвани източници

- S. Bosworth and M. Kabay, Computer security handbook, 1st ed. New York: John Wiley & Sons, 2002.
- Y. Xiang, Cyberspace safety and security, 1st ed. Heidelberg: Springer, 2012.
- https://www.calyptix.com/hipaa/top-5-cyber-security-frameworks-in-healthcare/
- https://securityboulevard.com/2020/02/cybersecurity-frameworks-in-healthcare-and-how-to-adopt-them/
- https://ignyteplatform.com/top-7-healthcare-cybersecurity-frameworks/
- https://www.legalreader.com/5-most-commonly-used-cybersecurity-frameworks-healthcare/