РОЗРОБКА ЗАХИСНОЇ ПРОГРАМИ З КІБЕРБЕЗПЕКИ ДЛЯ ПРОАКТИВНОГО ЗАХИСТУ З ДОПОМОГОЮ СТРУКТУРОВАНИХ ФРЕЙМВОРКІВ У ГАЛУЗІ КІБЕРБЕЗПЕКИ

Цей документ підготовлений на замовлення USAID. Його самостійно підготував партнер-виконавець «Каталісто» для діяльності USAID «Кібербезпека критичної інфраструктури в Україні». Погляди авторів, висловлені в цьому документі, не обов'язково відображають погляди USAID або уряду Сполучених Штатів.

МОДУЛЬ 4 - ВСТУП

Той факт, що в сучасному світі бізнес дуже сильно залежить від Інтернету, зумовлює необхідність для кожної організації, незалежно від її розміру та галузі, захистити свої підприємства від зловмисних впливів, внутрішніх загроз та інших ризиків, пов'язаних із кібербезпекою. Стоїть лише питання «коли», а не «якщо» ваша організація стане об'єктом кібератаки.

На щастя, фреймворки з кібербезпеки було розроблено таким чином, що вони включають в себе найкращі практики, стандарти та довідники, укладені для подолання ризиків та боротьби з небезпеками, і таким чином ви можете захистити ваші найцінніші активи: людей, власність та дані.

Навіть якщо ви не зобов'язані дотримуватись якихось особливих правил, має зміст налагодити активне подолання ризиків у вашому бізнесі. Усі фреймворки включають вказівки щодо гігієни у галузі кібербезпеки, такі як ефективне управління активами та інвентарем, планування на випадок виникнення неочікуваних ситуацій, захист персоналу, контроль доступу до системи, обізнаність персоналу та навчання, а також інші подібні речі.

Щоб підготуватися до наслідків кіберінциденту, фреймворки пропонують інструкції з реагування на інцидент, якими ви можете слідувати, щоб виявити та спробувати зменшити завдану шкоду. Встановлення фреймворку може не лише допомогти вашій організації слідувати найкращим практикам, але також запровадити сувору дисципліну у вашій організації.

ФРЕЙМВОРКИ ТА СТАНДАРТИ NIST (НАЦІОНАЛЬНОГО ІНСТИТУТУ СТАНДАРТІВ І ТЕХНОЛОГІЙ США)

NIST є агенцією уряду США, котра розробила кілька корисних фреймворків для підтримки кібербезпеки, що є основою для більшості інших фреймворків. Вони детально описані у спеціальних публікаціях (SPs), і пропонують особливі види контролю та найкращі практики, котрі можуть бути використані як у державному, так і у приватному секторах для досягнення певної цілі, описаної у кожній такій публікації.

NIST SP 800-37, фреймворк управління ризиками для інформаційних систем та організацій: підхід до безпеки та секретності, що базується на життєвому циклі системи (відомий як RMF). Він побудований навколо семи кроків: підготувати, внести до певної категорії, відібрати, впровадити, оцінити, авторизувати та перевірити. Цей процес допомагає організаціям розставити правильні пріорітети в управлінні ризиками шляхом оцінки, відстежування та ідентифікації цих ризиків.

NIST SP 800-53, Контроль захисту секретності для інформаційних систем та організацій є фреймворком, що добре себе зарекомендував. Він фокусує увагу на контролі секретності та визнанні того, що саме секретність є критичним моментом у сфері кібербезпеки.

NIST SP 800-171, Захист контрольованої некласифікованої інформації у нефедеральних системах та організаціях, фокусується на підтримці організацій, котрі зберігають, передають та обмінюються контрольованою некласифікованою інформацією (англ. Controlled Unclassified Information CUI) [1]. NIST 800-171 спрямований на те, щоб

допомогти нефедеральним організаціям, які ведуть бізнес з федеральним урядом, захистити конфіденційність CUI. Це інструкції для будь-якої організації для захисту своїх даних та даних своїх клієнтів.

Фреймворк кібербезпеки NIST, відомий як CSF, концентрує в собі функції кіберзахисту, необхідні для того, щоб обмежити ризики та зберегти активи. Ці функції є наступними: ідентифікувати, захистити, визначити, відреагувати та надолужити. Фреймворк задумано для такого використання, при якому організації можуть самі створити програму кібербезпеки, яка підходить для їхніх ризиків, ситуацій та вимог. Тоді вони можуть розставити пріоритети своїх інвестицій та максимізувати витрачання коштів на найбільш ефективне управління ризиками.

ВПРОВАДЖЕННЯ ФРЕЙМВОРКУ

Це безумовно може бути дуже складним завданням – визначитися з фреймворком та впровадити його ефективно. Деякі фірми можуть мати для цього ресурси, але потребуватимуть допомоги з інтерпретацією директив при впровадженні їх у свою організацію. Іншим фірмам може знадобитись зовнішній експерт для керування усім процесом.

Фірми, котрі виступають третіми особами в управлінні ризиками, можуть бути корисними в обох випадках, даючи поради бізнесам, з чого почати та який фреймворк обрати, щоб отримати більше користі.

Найголовніше, у чому може допомогти фірма, що займається управлінням ризиками, це розпочати з аналізу розрахунків. Цей аналіз оцінює існуючий стан кібербезпеки вашої фірми та визначає, як досягти стану, який повинен бути. Зовнішні експерти визначать, прорахують та розставлять пріоритети ризиків вашої організації, а також її слабкі місця, і порадять, як правильно виправити ситуацію. Це може включати поради щодо найбільш відповідного фреймворку, котрий допоможе якнайкраще захистити людей, власність та дані вашої організації та максимізувати ефективність ваших інвестицій у кібербезпеку. Коли вихідні дані визначено, і ви знаєте, куди спрямувати зусилля, ви починаєте використовувати інструкції обраного вами фреймворку, щоб протягом тривалого періоду часу порівнювати стан справ у вашій організації відносно цієї точки відліку.

Знаючи про складність, креативність та рівень кіберзлочинів, з якими зіштовхується організація, важливо використати кожен доступний інструмент для боротьби з цими атаками. Впровадження перевіреного фреймворку кібербезпеки, котрий відповідає потребам та ризикам вашого бізнесу, дає вам засоби для захисту вашого підприємства від небезпек, котрі стоять перед вами сьогодні, та будуть продовжувати загрожувати вам у майбутньому.

ФРЕЙМВОРК З КРИТИЧНИХ ЕЛЕМЕНТІВ УПРАВЛІННЯ БЕЗПЕКОЮ (CSC)

Головна проблема, з якою зіштовхуються професіонали у сфері IT безпеки, це те, що небезпеки еволюціонують так само швидко, як і технології. Технології є для бізнесу життєво важливими, особливо коли багато спеціалістів працюють за межами стандартного офісу, і це створює додаткові слабкі місця у системах захисту.

CIS Фреймворк з критичних елементів управління безпекою використовується настільки широко, що його можна знайти у різних директивах, а саме:

- CIS CSC
- CIS 20 / 18 (Найновіша версія)
- CCS CSC
- SANS Top 20
- CAG 20

Ключовим моментом для зменшення ризиків є наявність міцної бази, на основі котрої створюються специфічні протоколи з кібербезпеки для бізнесу чи індустрії. Інструментарій CIS 18 (CSC) є такою базою.

ЩО ЯВЛЯЮТЬ СОБОЮ CIS КРИТИЧНІ ЗАХОДИ БЕЗПЕКИ

CSC є інформаційною базою дієвих найкращих практик, розроблених Центром Інтернет безпеки (CIS) та Інститутом SANS. Ці дані надані великою кількістю професіоналів у сфері кібербезпеки, конденсовані та роз'яснені експертами даної індустрії. Ця інформація представлена у такому форматі, що її можна адаптувати для будь-якої організації, щоб протидіяти найпоширенішим формам кібератак та захистити дані та активи.

Ці базові принципи дають можливість професіоналам у сфері IT реагувати швидко та ефективно на зростання проблем у сфері безпеки. Це дозволяє організаціям знизити ризики у кіберпросторі.

ЯК ВПРОВАДИТИ CIS CCS У ВАШІЙ ОРГАНІЗАЦІЇ?

Усі організації повинні постійно здійснювати певну навігацію ризиків та власної гнучкості. У стандартах індустрії часто визначено, на яку глибину організації слід занурюватися у дослідженні цих питань, але рідко пояснено, як це робити. CIS CSC є набором найкращих практик, у якому є рекомендації, як боротися із найбільш популярними кіберзагрозами. Ці рекомендації можна використати у будь-яких організаціях.
CSC поділено на три групи впровадження. Кожен набір заходів є послідовністю, що базується на потребах організації:

- **Базове впровадження** стосується заходів 1 – 6 і є рекомендоване для усіх організацій. Ці шість заходів можуть бути впроваджені за наявності традиційних ресурсів і забезпечать базовий рівень захисту. Навіть найменші організації можуть його використати.
- **Ґрунтовне впровадження** стосується базових засобів та заходів 7 – 16 і є рекомендоване для організацій середнього розміру, які мають більше ресурсів та професіоналів у сфері кібербезпеки, щоб впровадити стандарти безпеки.

- **Організаційне впровадження** стосується усіх 18 заходів з безпеки і розроблене для розвинутих організацій, котрі володіють великими ресурсами та мають серйозну експертну групу у сфері кібербезпеки.

Завдяки сегментації заходів згідно ресурсів та рівня експертності, організація має можливість обрати те, що найкраще підходить для її інфраструктури.

НАВІЩО ВИКОРИСТОВУВАТИ ЗАХОДИ CIS ДЛЯ БЕЗПЕКИ ТА ВІДПОВІДНОСТІ?

CIS top 18 CSC є еволюцією світових знань від IT професіоналів, котрі щодня глибоко вникають у проблеми кібербезпеки.

Результати від користування CSC є феноменальними. Дослідження показують, що 85% кібератак можуть бути відбиті при використанні лише базового впровадження CSC. Використання організаційного впровадження усіх 18 заходів CSC дає приголомшливий рівень успіху - 97%.

Користуючись наведеними вище найкращими практиками, організація може мати сильну базу з кібербезпеки, котра вже довела свою цінність. Ця база є ідеальною для побудови системи безпеки при наявності будь-яких додаткових специфічних вимог певної індустрії.

ЯК ЗАХОДИ CSC ПРАЦЮЮТЬ З ІНШИМИ СТАНДАРТАМИ?

Заходи CSC є сумісними з іншими засобами, тому що вони являють собою ефективні найкращі практики, що охоплюють великий спектр загроз. Специфічні стандарти певної індустрії та ідеології інструментарію кібербезпеки зростають та еволюціонують паралельно з технологіями, і CSC допомагають організаціям встигати за швидкими змінами середовища кібербезпеки.

Наприклад, Акт про конфіденційність споживачів Каліфорнії (CCPA) та Акт про загальний захист даних (GDPR) вимагають від організацій, щоб вони забезпечили належний рівень безпеки для захисту приватних даних їхніх покупців. Крім того, Акт кібербезпеки Інтернету речей (IoT) вимагає під'єднання пристроїв для забезпечення мінімального рівня кібербезпеки. Використання заходів CIS Top 18 CSC дозволяє організаціям досягти цих порогів безпеки.

Також CSC є добре сумісними з іншими відомими стандартами безпеки таких організацій та нормативних документів як:

- Національний інститут стандартів та технологій (NIST)
- Міжнародна організація стандартизації (ISO)
- Стандарти безпеки даних індустрії платіжних карток (PCI-DSS)
- Акт про підзвітність та мобільність страхування здоров'я (HIPAA)
- Завдання управління для інформаційних і суміжних технологій (COBIT)
- Акт 2014 року про модернізацію системи безпеки федеральної інформації (FISMA)

- Стандарти захисту критичної інфраструктури NERC (NERC CIP)
- Наглядова рада фінансових урядових установ (FFIEC)
- Департамент державної безпеки, Відділ діагностики та пом'якшення ризиків (DHS CDM)
- Інструкція з управління мережею Національної агенції з кібербезпеки (NSA MNP)
- Стандартний набір інструментів для безпеки та захисту даних (NHS DSP Toolkit)

Заходи CSC є дуже важливими для допомоги організаціям, яким потрібно відповідати цим комплексним стандартам та вимогам індустрії.

ОГЛЯД ЗАХОДІВ CIS

Базові заходи CIS

Базовий рівень впровадження стосується заходів 1 – 6 і забезпечує мінімальний рівень кібербезпеки, котрого повинні досягти усі організації, щоб бути готовими до кібератак.

Захід 1: Інвентаризація та контроль за активами підприємства

Знання того, хто і що використовує мережу, є ключовим моментом для запобігання неавторизованому доступу. Це включає ведення детальної інвентаризації за допомогою активного та пасивного підходів та використання контролю доступу. Поглиблений огляд усіх пристроїв, які використовують мережу організації, забезпечує першу лінію захисту.

Захід 2: Інвентаризація та контроль активів програмного забезпечення

Програмне забезпечення слід інвентаризувати та перевіряти в такий спосіб, який дозволить організації побачити, що саме з програм було встановлено, хто проводив встановлення, що ця програма зараз робить. Обов'язковим є впровадження листка авторизації, прав на встановлення та контролю цілісності. Так само, як технічне обладнання, програмне забезпечення може бути використане як слабке місце для втручання у захищену мережу.

Захід 3: Захист даних

Розробіть процедури та технічні заходи для ідентифікації, класифікації, безпечної обробки, збереження та розміщення даних.

Захід 4: Безпечна конфігурація активів та програмного забезпечення підприємства

Оновіть типові конфігурації та автоматизуйте процеси для управління ними. Управління конфігураціями є необхідним для блокування зайвих ризиків, які можуть бути використані хакерами.

Захід 5: Управління акаунтами

Використовуйте процеси та інструменти для встановлення та подальшого керування процесом авторизації акаунтів користувачів та адміністраторів, а також доступів до сервісів підприємства та програмного забезпечення.

Захід 6: Управління доступом

Користуйтеся процедурами та інструментами для створення, призначення, управління та анулювання доступів та привілеїв для користувачів, адміністратора, а також для обслуговування акаунтів, активів та програмного забезпечення організації.

Ґрунтовні заходи CIS

Ґрунтовний рівень впровадження стосується також заходів 7 – 18 і визнається придатним для організацій середнього розміру, котрі потребують захисту систем на дещо вищому рівні, ніж базовий.

Захід 7: Безперервне управління вразливостями

Розробіть план довготривалого оцінювання та відстежування слабких місць у системі захисту всіх активів підприємства для того, щоб зменшити можливості проникнення для хакерів. Досліджуйте державні та приватні джерела інформації, щоб дізнаватись про нові загрози та вразливі місця.

Захід 8: Управління журналом подій

Збирайте, переглядайте та зберігайте журнали подій (логи), це може допомогти визначити атаку, зрозуміти її та захиститися.

Захід 9: Захист електронної пошти та веб-браузера

Покращуйте захисти та способи виявлення небезпек, що можуть надійти через електронну пошту та веб, оскільки це можливості для хакерів, щоб маніпулювати поведінкою людей через особисте спілкування.

Захід 10: Захист від вірусів

Запобігайте або контролюйте встановлення, поширення та використання вірусних додатків, кодів або документів в активах підприємства.

Захід 11: Відновлення даних

Встановіть та дотримуйтесь практик з відновлення даних, які допоможуть відновити активи підприємства до рівня, який був до інциденту.

Захід 12: Управління інфраструктурою мережі

Встановіть, впровадьте та активно керуйте (відстежуйте, переглядайте звіти, коректуйте) роботою мережевих пристроїв, щоб запобігти атаки хакерів через вразливі місця у системі захисту мережі, її службах та точках доступу.

Директива 13: Моніторинг та захист мережі

Оперуйте процесами та інструментами для встановлення та підтримки належного моніторингу роботи мережі та її захисту від загроз, які можуть з'явитися через інфраструктуру мережі підприємства та базу користувачів.

Директива 14: Обізнаність у питаннях кібербезпеки

Встановіть та підтримуйте програму обізнаності у кібербезпеці, щоб впливати на поведінку працівників на робочих місцях. Вони повинні бути свідомими та мати відповідні навички, щоб знизити ризики у кібербезпеці підприємства.

Директива 15: Управління провайдерами послуг

Розробіть процедуру оцінювання провайдерів послуг, які мають доступ до важливих даних або є відповідальними за важливі IT платформи або процеси підприємства, щоб переконатися, що ці провайдери належним чином захищають ці платформи та дані.

Директива 16: Безпека додатків та програм

Хакери використовують чинні посвідчення осіб, і це проблема, яку потрібно озвучувати. Загальною рекомендацією є подвійна ідентифікація для входу в акаунт.

Директива 17: Управління реагуванням на інцидент

Встановіть програму для розробки та підтримки здатності реагувати на інциденти (прикладом можуть бути різні політики, плани, процедури, визначені ролі, тренінги та комунікації), щоб підготуватися, вчасно визначити та зреагувати на атаку.

Директива 18: Тести на проникнення та тренування Червоної команди

Визначте місця можливого проникнення та усуньте їх, як тільки знайдете. Продовжуйте тестування та виправлення, оскільки вектор атак змінюється.

БЕЗКОШТОВНІ ЗАСОБИ АКТИВНОГО ЗАХИСТУ

В той час як уряди та приватні компанії ведуть дебати щодо Наступального підходу до кібербезпеки, перехід до практики є дуже швидким. Набір інструментів із відкритими джерелами інформації стає доступним на публічному домені для приватних компаній, котрі вирішили переслідувати порушників.

Модель «активного захисту» набирає численну підтримку у приватному секторі, і це підштовхує спеціалізовані компанії, такі як CrowdStrike, HBGary та Mykonos до складання комерційної пропозиції.

Основами методів активного захисту є все від інструментів, схожих на «пастки», щоб спіймати потенційних зловмисників та простежити за ними. Здатність привернути увагу хакерів, вивчаючи їхні тактики, є надзвичайно важливою. З боку захисту існують різні опції, наприклад, компанія може безпосередньо атакувати підозрюваних у злочині, який їм загрожує, або може вибрати інший шлях: обмежити свій активний захист,

заважаючи хакерам, наприклад, підриваючи їхню розвідувальну діяльність і навіть точно визначаючи їхнє фізичне розташування.

Дмітрій Альперович, співзасновник та технічний директор компанії CrowdStrike відзначає, що активний захист передбачає дії, спрямовані на визначення загроз у реальному часі та ідентифікацію особи зловмисника, поширення неправдивої інформації та руйнування систем нападника як крайній захід.

"Захисні техніки у чистому вигляді… не будуть працювати ефективно, якщо ворог має високий рівень професіоналізму і рішуче налаштований проникнути у систему, він знайде варіант як це зробити. Тож вам потрібно знайти інші способи їх стримувати. Це передумова активного захисту ", - зазначає Альперович.

Іншою можливістю є проведення розвідувальної діяльності серед потенційних зловмисників, намагаючись ідентифікувати шляхи їхніх дій та цілі/інформацію, яку вони використовують. Фірма CrowdStrike, що працює у галузі кібербезпеки, планує випустити різноманітні засоби для активного захисту. Компанія анонсувала розповсюдження поліморфної програми для аналізу та декодування, а також безкоштовних інструментів для стеження за атакувальниками через Tor.

Цей ринок є дуже плідним. Експерти з кібербезпеки Джон Странд, Пол Азадурян, Етан Робіш та Бенджамін Донеллі пропонують набір інструментів Linux distro для захисту через напад.

ADHD є класифікацією засобів активного захисту із попередньо розробленими інструментами для контратак, що можуть бути використані для втручання в систему з допомогою відбитків пальців атакувальника.

Дистрибутив включає наступні інструменти захисту:

- *Артилерія (Artillery)*
- *Капкан для ведмедя (BearTrap)—відкриває тригерні порти власника системи для привернення уваги хакерів, автоматично помічає їх та заносить до чорного списку.*
- *Зняття маски (Decloak) – для ідентифікації реальної IP адреси користувача, навіть через проксі.*
- *Медоїд (Honey Badger) – для визначення фізичного розташування користувача.*
- *Нова (Nova) (Заплутування мережі та віртуалізована система анти-зондування) – визначає проведення розвідувальних робіт в мережі та надає хакеру неправдиву інформацію щодо кількостей та типів систем у цільовій мережі, використовує мережу віртуалізованих пасток. Нова не використовує визначення вірусів на основі підпису, натомість вона створює системи пасток для атакувальника, щоб він з ними взаємодіяв, та попереджає системного адміністратора про підозрілу активність.*

- *Павукова пастка (The Spidertrap) – є набором вебсторінок, котрі можуть умисно або неумисно бути використані, щоб примусити пошукову програму або бота здійснити нескінченну кількість запитів, або призвести до руйнування пошукової програми, якщо вона не якісно сконструйована.*

- *Жучок (Web Bug Server) – вставляє системного «жучка» всередину документу, який може бути використаний для приховування HTML коду, що неодмінно викриє IP адреси та іншу інформацію про хакера.*

“Ми хочемо змінити рахунок на нашу користь, не вдаючись до атак у відповідь,” – відмічає Странд. Експерт заперечує легітимність таких інструментів, вважаючи, що пропозицію адресовано експертам з кібербезпеки, котрі підтримують ідею законного включення їх у використання. «Люди запитують: «Чи це законно?» Ми можемо відповісти: «Майже. Дуже близько.»

“Ми не можемо проникати у їхні комп’ютери та копирсатися у їхніх файлах, навіть якщо вони є поганими хлопцями або злочинцями. Вони мають право на захист своєї інформації, і ми намагаємося не перетинати цю межу” – зазначив Странд.

МАТЕРІАЛИ ТА ПОСИЛАННЯ

1. Модуль_4_Whitepaper1-LM-White-Paper-Intel-Driven-Defense
2. https://www.cisecurity.org/controls/
3. https://www.cisecurity.org/white-papers/cis-controls-v8-mapping-to-nist-csf/
4. https://www.cisecurity.org/white-papers/cis-controls-v8-mapping-to-nist-800-53-rev-5/
5. https://www.cisecurity.org/white-papers/cis-controls-v8-cybersecurity-maturity-model-certification-mapping/