СТВОРЕННЯ ТА ВПРОВАДЖЕННЯ ПРОГРАМИ НАВЧАННЯ ТА ТЕСТУВАННЯ ПРАЦІВНИКІВ У СФЕРІ 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 2 - ВСТУП

Ви можете встановити складні паролі, кодування диску та використовувати три різні типи програм для захисту, та ніщо з цього не матиме значення, якщо ви не докладете максимум зусиль до роботи із найголовнішим складником вашої системи безпеки – вашими працівниками. Хоча зазвичай це стається без злого наміру, та саме через працівників у системі безпеки виникають інциденти через фішинг атаки, які налічують до 43 відсотків усіх випадків витоку інформації. Крім технічних засобів, загальна Програма тренінгів, спрямованих на підвищення обізнаності у кібербезпеці (SAT) є надзвичайно важливою, коли вона є частиною вашого плану по безпеці. В той час, як багато організацій проводять формальні тренінги та семінари, розсилають оновлення електронною поштою, і навіть екзаменують своїх працівників на предмет їхньої обізнаності з питань кібербезпеки, існує одне питання, на котре лідерам в галузі IT дуже важко відповісти… а саме: це дійсно працює?

Що таке Навчання, спрямоване на підвищення обізнаності у кібербезпеці (SAT)?

Навчання, спрямоване на підвищення обізнаності у кібербезпеці є процесом викладання працівникам належної інформації щодо найкращих практик та нормативів у галузі безпеки, політики компанії у цій сфері та загальних інструкцій. SAT є програмою, що повинна забезпечити навчання працівників на регулярних засадах, щодо того, як їм найбільш ефективно захистити себе та бізнес від потенційно шкідливих втручань. Забезпечення працівників знаннями та подальше нагадування про можливі наслідки від порушення цілісності системи безпеки повинно стати стовпом, на якому триматиметься уся система правил безпеки компанії.

НАВІЩО ТА ЯК САМЕ НАВЧАТИ ПРАЦІВНИКІВ?

Надання працівникам знань, які допоможуть їм розпізнати кіберзагрози, може бути найважливішим компонентом кібербезпеки вашої організації. Навчання, спрямоване на підвищення обізнаності у кібербезпеці, тренує у працівників розуміння того, якими є вразливі місця організації та які загрози можуть поставати перед бізнес процесами. Вашим працівникам неодмінно потрібно бути обізнаними щодо їхніх обов'язків та відповідальності при користуванні комп'ютером у бізнес мережі.

Тренінги для новачків та регулярні навчальні курси, спрямовані на поновлення знань та повторення, повинні бути обов'язковими для популяризації культури безпеки у вашій організації. Тренінги для працівників повинні включати в себе (та не обмежуватися цим):

1. Відповідальність за дані, що належать компанії

Слід наполегливо і тривало наголошувати на критичній важливості безпеки даних та відповідальності кожного працівника за захист даних компанії. Ви і ваші працівники мають юридичні зобов'язання поважати і захищати секретність інформації, а також її цілісність та конфіденційність.

2. Управління документообігом та Процедури інформування

Працівники повинні знати запроваджену у вас процедуру звітування про інцидент на той випадок, якщо комп'ютер працівника інфіковано вірусом, або він працює з відхиленнями від

норми (наприклад, непояснимі помилки, процеси відбуваються занадто повільно, наявні зміни у конфігурації робочого стола і т.ін.). Вони повинні бути навчені вирізняти легітимне повідомлення із застереженням або сигнал тривоги. У таких випадках працівники повинні невідкладно звітувати про інцидент, щоб ваша IT команда могла стримати та дослідити цю загрозу.

3. Паролі

Навчіть своїх працівників створювати надійні паролі. Паролі повинні бути такими, щоб неможливо було легко здогадатися, які саме паролі встановлено, та водночас вони повинні легко запам'ятовуватися, щоб не було необхідності їх записувати. У вашій компанії повинна бути налагоджена система автоматичної розсилки нагадувань працівникам про потребу змінити паролі.

4. Недозволене програмне забезпечення

Повідомте своїх працівників про те, що вони не мають права інсталювати неліцензоване програмне забезпечення на жоден комп'ютер компанії. Завантаження неліцензованих програм може призвести до завантаження зловмисних програм, котрі спровокують кібератаку і пошкодять дані вашої компанії.

5. Користування інтернетом

Навчіть своїх працівників уникати посилань, що приходять електронною поштою або з'являються онлайн з ненадійних джерел. Такі посилання можуть надати зловмисним програмам доступ до вашої системи, що призведе до інфікування комп'ютера та викрадення даних компанії. Ваша компанія також повинна встановити правила безпечного користування інтернетом та обмежити працівників у користуванні ним на робочому місці.

6. Електронна пошта

Відповідальне користування електронною поштою є найкращим захистом від викрадення даних. Працівники повинні знати, що таке шахрайство, та не відповідати на повідомлення електронною поштою, які вони не можуть ідентифікувати. Навчіть своїх працівників приймати листа електронною поштою, якщо:

- Лист надійшов від когось, кого вони знають.
- Лист надійшов від когось, від кого вже надходили листи раніше.
- Є чимось очікуваним.
- Лист не виглядає таким, що відрізняється від інших, наприклад, містить незвичний порядок букв або дивні символи.
- Лист пройшов перевірку вашою антивірусною програмою.

7. Соціотехніка (тактика зловмисного проникнення у систему) та фішинг

Навчіть своїх працівників визначати кіберзлочини та ризики, що загрожують інформаційній безпеці, включно із соціотехнікою, інтернет-шахрайством, фішингом та ризиками від відвідування вебсайтів в інтернеті.

8. Політика соціальних медіа

Навчіть своїх працівників дотримуватися вашої політики щодо соціальних медіа, та ознайомте з інструкціями щодо користування корпоративною електронною поштою для реєстрації, створення дописів та отримання інформації через соціальні медіа.

9. Мобільні пристрої

Донесіть до своїх працівників інформацію щодо вашої політики користування мобільними пристроями, які є власністю компанії, а також тими, що є у персональній власності.

10. Захист комп'ютерів

Навчайте своїх працівників захищати їхні комп'ютери від зловмисного втручання шляхом їх блокування та зберігання їх у безпечному місці. Слід регулярно здійснювати резервне копіювання важливої інформації, ці копії також слід зберігати у безпечному місці. Усі ваші працівники несуть відповідальність за підтримку актуальності антивірусних програм на ПК компанії.

11. Створення культури кібербезпеки

Культура кібербезпеки довший час розглядалася як Священний Грааль для керівників, що займаються кібербезпекою. Такої культури об'єктивно важко досягнути.

Для навчань, спрямованих на підвищення обізнаності у сфері кібербезпеки, хтось повинен керувати процесом у правильному напрямку.

Створення культури безпеки означає надання безпеці цінності у вашій організації чи в бізнесі. Навчання, спрямоване на ситуаційну обізнаність (розуміння того, чому хтось може зазнати ризиків), а також популяризація професійних та життєвих цінностей є гарним методом залучення свідомих людей у команду.

Тренінгові платформи можуть допомогти у моніторингу та розвитку культури кібербезпеки, роблячи людей вашою першою лінією захисту.

12. Бути представником соціально відповідального бізнесу

Як показали у 2017 році WannaCry та NotPetya, кібератаки можуть поширюватися неймовірно швидко. Чим більше мереж було вражено, тим більше стає інших мереж, які тепер у групі ризику. Одна слабка сторона мережі робить вразливою усю систему.

Відсутність навчання кібербезпеці в одній організації робить іншу організацію більш вразливою. Це як залишити двері своєї домівки відчиненими, а всередину покласти ключі від сусіднього помешкання.

Навчання кібербезпеці є важливим не лише для вас. Воно важливе для ваших клієнтів, ваших постачальників та усіх, хто контактує з вашою комп'ютерною мережею.

ЯК ЦЬОГО ДОСЯГТИ?

1. Вчитися на прикладах

Хороші звички у сфері безпеки починаються з менеджменту. Якщо у власника паролі, написані на стікері, приклеєному до монітора, а сам комп'ютер залишається без нагляду і незаблокованим протягом обідньої перерви, або незаблокований лептоп стоїть на його столі усю ніч, чому б тоді працівникам поводитися по-іншому? Найкращий шлях привити працівникам правильні звички щодо дотримання заходів кібербезпеки – це самостійно змоделювати їх як менеджер. Дослівно дотримуйтесь протоколів кібербезпеки, а інакше ви дасте іншим підстави їх не дотримуватися.

2. Щодня розсилати маленькі підказки щодо кібербезпеки

Розміщення на столі кожного працівника довідника з політики кібербезпеки вашої компанії на сто сторінок дасть надійну гарантію, що його ніколи ніхто не почитає і не використає. В той час, як формальна документація відіграє свою роль, невеличкі поради та підказки щодо кібербезпеки будуть більш ефективними як для навчання, так і для нагадування про корисні звички щодо кібербезпеки. Ці підказки можна розсилати щодня електронною поштою у вигляді одного пункту політики кібербезпеки на день, або пояснювати один термін з цієї галузі (наприклад, що таке фішинг?), або фокусувати увагу на якійсь нещодавній події у сфері кібербезпеки з новин, щоб інформація про ризики або втрати добре запам'яталася.

3. Суворо наполягати на дотриманні політики кібербезпеки

В багатьох компаніях, особливо у невеликих, звичною справою є випущення протоколів кібербезпеки з уваги. Ви можете (суворо) вимагати особистої присутності кожного при заміні пароля, але коли часу обмаль і працівники зайняті, відділ IT може оминути це розпорядження і здійснити зміну пароля по телефону. Дуже обмежено надавайте дозвіл на таку процедуру, навіть якщо на протилежному кінці дроту хороший друг і немає проблем з ідентифікацією. Переконайтеся, що і працівник і IT відділ не сприймають це як вашу прискіпливість, і розуміють, що це захист від зловмисників, котрі шукають слабкі місця у вашій системі кібербезпеки.

4. Тестування працівників

Говорити працівникам, щоб вони були обережними із соціотехнікою – це ще не все. Ви повинні також знати, чи дійсно вони дотримуються ваших інструкцій, коли їм телефонують хакери. Чому б не перевірити їх, змоделювавши ситуацію, схожу на реальність? Для цього можна оплатити послуги експерта з кібербезпеки або реалізувати це власними силами. В будь-якому разі, вам потрібно буде подзвонити працівнику, котрий має доступ до важливої інформації – чи це паролі, чи дані з клієнтської бази – і спробувати примусити його порушити протокол кібербезпеки. Якщо це вдасться, ви знатимете, що слід провести додаткове навчання.

5. Зробити засоби безпеки легко доступними

Працівники не будуть користуватись такими інструментами, як засоби шифрування, VPN та сканер вірусів, якщо вони не будуть широкодоступними або з ними буде складно працювати.

Зробіть ці інструменти доступними за замовчуванням на кожному комп'ютері в організації. Поширюйте цю концепцію на все, що стосується безпеки, включаючи шухляди та шафи для файлів, які блокуються, а також подрібнювачі паперу. У працівників часто є доступ до шредерів або інших пристроїв для безпечного знищення документів, але вони ними не користуються, тому що доступ до них ускладнений, або вони розташовані на занадто великій відстані від робочого стола. Загальна теорія: зроби легкою адаптацію до дій, що забезпечують захист, і працівники будуть ці дії виконувати.

ЯК ЗНАТИ, ЩО МОЯ ПРОГРАМА НАВЧАННЯ, СПРЯМОВАНА НА ПІДВИЩЕННЯ ОБІЗНАНОСТІ У КІБЕРБЕЗПЕЦІ ПРАЦЮЄ?

Програма SAT може бути досить дорогою. Багато управлінців мають застереження щодо витрачання значних коштів на навчання, присвячені кібербезпеці, тому що складно перевірити, що воно дійсно ефективне. Один з методів, до якого вдаються сучасні бізнеси, і по якому можна отримати статистичні підрахунки щодо ефективності навчання з кібербезпеки за прийнятні кошти – це тестування з симуляцією фішингу.

1. Тест із симуляцією фішингу

Такий тест полягає у симульованих електронних листах, метою яких є обманним шляхом примусити ваших працівників відкрити такого листа, що є потенційно шахрайським, перейти за сумнівним посиланням, внести інформацію з посвідчення особи на фальшивій сторінці, розробленій так, щоб вона виглядала, як справжня (наприклад, LinkedIn, DropBox, PlayStation і т.д.). Ці листи виглядають так, наче надійшли з відомого джерела, наприклад, від президента компанії, добре відомого працівника або клієнта, з відомого веб-сайту, або навіть з банку чи державного органу. Ці симулятори побудовані з врахуванням загальноприйнятих інструкцій щодо кібербезпеки у сфері електронного листування, і працюють таким чином, що працівники, які розуміють, як працює інформаційна безпека, пройдуть цю перевірку. Ці симулятори надзвичайно корисні, оскільки одразу вимальовують для вас реальну картину рівня обізнаності у кібербезпеці у вашій компанії . У звіті буде зазначена інформація про те, хто з працівників був обманутий під час цього тесту, включно з інформацією про те, хто вніс свої особисті дані на фальшивій сторінці. Крім цього, більшість таких фішингових симуляторів дають зрозуміти працівникам, які провалили тест, де саме вони схибили і що їм натомість слід було робити.

Симулятивний фішинг тест може бути відносно дешевим, мати додаткову перевагу у тому, що він одночасно навчає вашу команду діяти правильно наступного разу, поки ви шукаєте інші слабкі місця у вашій системі кібербезпеки.

2. Перевірка надійності паролів (PET)

Паролі є однією з найважливіших частин системи кібербезпеки, та досі багато працівників часто ігнорують підказки та інструкції щодо створення паролів. Нещодавнє дослідження, проведене Thycotic, показало, що 30% людей досі використовують дати свого народження, адреси, імена домашніх улюбленців або дітей для створення своїх паролів. А це величезне «ні-ні-ні» для паролів.

Одним із швидких і недорогих методів перевірки вашого Плану навчання, спрямованого на підвищення обізнаності у кібербезпеці – це залучення команди консультантів третьої сторони для проведення PET. Така перевірка полягає в тому, що добре навчений та кваліфікований

професіонал з кібербезпеки діє як хакер і намагається розсекретити паролі працівників звичайними хакерськими методами, такими як метод прямого підбору. Результати такої перевірки являють собою дружній звіт, який показує вам, скільки паролів було зламано під час проведення тесту, і в чому саме схибили працівники, створюючи свої паролі. Це допоможе вам і вашій команді зміцнити свою політику щодо паролів, якщо це потрібно, а також на що звернути увагу під час наступного навчання, спрямованого на підвищення обізнаності у кібербезпеці.

3. USB тест

Соціотехніка – це коли кібер злочинець намагається примусити працівника встановити вірусну програму або розголосити секретну інформацію. Однією з поширених форм соціотехніки є отримання доступу через USB ключі або флешки, на яких міститься вірус, які залишають умисно у незаблокованому пристрої або дають комусь покористуватися. USB накопичувачі дещо вийшли з моди через розвиток Хмарного сховища, однак люди досі зберігають важливу інформацію на USB флешках.

USB тест є такою формою тестування обізнаності у соціотехніці, коли «підробну» флешку залишають десь поблизу, наприклад на паркінгу або у кімнаті для відпочинку, чи навіть на робочому столі працівника. Цей USB ключ або флешка містить програму, яка швидко дасть вам знати про те, коли і куди її було під'єднано. Це дасть можливість викрити працівників, котрі не повністю розуміють небезпеку від користування невідомим USB накопичувачем.

4. Перевірка середовища

Багато нехтувань системою безпеки стаються через звичайні помилки, такі як залишання комп'ютера на робочому столі без блокування, залишання важливої інформації у принтері на невизначений період часу, та недотримання правил поведінки відвідувачів. Обійдіть свій офіс, або краще попросіть зробити це кваліфікованого консультанта з кібербезпеки, і задайте наступні запитання:

- Чи бачите ви ПК, у які користувачі залогувалися і залишили їх без уваги?
- Чи у принтері лежать документи без уваги?
- Чи перебуває на вашій території підрядник без нагляду або без бейджа відвідувача?
- Чи користуються працівники недозволеними методами поширення файлів, такими як DropBox або USB накопичувач?
- Чи використовує хтось недозволені пристрої для роботи? (наприклад, лептоп, планшет, телефон і т.д.)
- Чи беруть працівники пристрої або матеріали додому?

Пам'ятайте, щоб кібербезпека була ефективною, вона повинна бути об'єктом відповідальності кожного. Отже переконайтеся, що ви доносите важливість Навчання, присвяченого обізнаності у кібербезпеці, вчасно та достатньо часто.

МАТЕРІАЛИ

1. Модуль _2_Whitepaper1-JL_Privacy_Training_White_Paper_2021
2. Модуль_2_Whitepaper2-Employee Training as a Tool for Cyber Security