Асоціація Благодійників України

Ольга Гужва, експертка з кібербезпеки та директорка з розвитку Асоціації Благодійників України (https://vboabu.org.ua/)

Ольга Гужва, має досвід роботи в зоні проведення бойових дій різної складності, в супроводі з військовими, парамедиками, гуманітарними місіями. Понад два роки роботи на лінії фронту, понад 30 проведених тренінгів для понад 300 учасників, в тому числі іноземців. (Проходила тренінги згідно з протоколами HEAT та BSAFE від Unated Nation, UN Peacekepeng Operation, Forth Global, Center for International Peace Operation.) Входить до експертнеї мережі DCN Global, Knowbe4 (USA)
guzhva(at)mediaexpert.group

«Кібербезпека – відповідальність кожного! Це не відповідні розроблені політики безпеки, це не загроза санкцій чи навпаки заохочення, це свідома поведінка кожного співробітника постійно підвищувати свою обізнаність та застосовувати отриманні знання на практиці».

Не всі, навіть в бізнесі, інвестують у навчання працівників кібербезпеці, а що вже казати про громадський сектор, що підтверджують дослідження Hornetsecurity (https://www.hornetsecurity.com/en/) навіть у випадку гібридних робочих місць. Такий формат залучення працівників в останні три роки є досить поширеним, особливо у громадському секторі. Наскільки усвідомлено підходять громадські та благодійні організації до питань кібербезпеки для віддалених співробітників і на що треба звернути увагу розглянемо далі.

Повномаштабне вторгнення, релокація працівників спричинили серйозний зсув до віддаленої роботи, особливо у проєктній роботі, що є найбільш поширеною у громадському секторі.

Станом на сьогодні близько 10% працівників в організаціях працюють з дому повний робочий день, разом з цим значна частина працює за гібридною моделлю. Хоча багатьом працівникам подобається гнучкість, слід звернути увагу на безпекові моменти використання пристроїв, які належать працівникам та організації, якщо такі передбачаються, незахищені з'єднання та неправильне використання пристроїв роблять організації вразливими до безлічі мережевих вторгнень. Тому навчання працівників кібербезпеці є вкрай важливим для громадських організацій, я б сказала, є обов'язковим.

Організації не проводять системного навчання з кібербезпеки для віддалених працівників, незважаючи на те, що більшість працівників мають доступ до критично важливих даних або працюють з чутливою інформацією.

Працівники, що працюють віддалено, та які мають доступ до критично важливих даних організації, не проходять регулярно навчання та не знають чіткого протоколу дій, що треба робити у разі інциденту.

Популярність гібридної роботи, а іноді вимушеність такого формату та пов'язані з нею ризики означають, що організації повинні надавати пріоритет навчанню та чіткому розумінню співробітниками, що робити у разі інциденту або як його розпізнати, щоб зробити віддалену роботу безпечною. Традиційні методи контролю та захисту виявилися не настільки ефективними коли співробітники працюють у віддалених місцях і більша відповідальність лягає персонально на співробітника. Адже поруч з робочими процесами та сеансами він може відкривати свої неперевірені ресурси або додатки. Організації повинні визнати унікальні ризики, пов'язані з віддаленою роботою, і активувати відповідні системи управління безпекою, а також надати співробітникам чітки протоколи як справлятися та реагувати на певні рівні ризиків.

Збільшення заходів щодо кібербезпеки віддаленої роботи особливо важливо щодо благодійних та громадських організацій, оскільки кіберзлочинці стають розумнішими. Ми спостерігаємо збільшення кількості атак на смартфони, оскільки хакери розуміють, що і особисті, і професійні дані можуть бути доступні, оскільки люди можуть і часто виконують роботу на персональних пристроях.

Відсутність знань збільшує ризик

Брак розуміння, впевненості та знань щодо кібербезпеки у працівників під час віддаленої роботи є основним ризиком. Також «неконтрольований обмін файлами» в різних месенджерах та додатках є поширеним джерелом інцидентів кібербезпеки організації.

Організації можуть зменшити ризики, пов'язані з кібербезпекою, шляхом підвищення рівня освіти та навчання. Навіть базове але системне навчання може значно покращити ситуацію.

Використання керування кінцевими точками

Обрати які ноутбуки, стаціонарні комп'ютери й інші кінцеві точки матимуть доступ до даних організації, а також отримувати відомості про ці пристрої.

Важливо мати надійні системи захисту працівників. Найчастіше основними джерелами інцидентів кібербезпеки є скомпрометовані кінцеві точки (тобто ті пристрої з яких працівники працюють) і скомпрометовані облікові дані (емейли, логіни та паролі тощо). Більшість співробітників використовують власні пристрої з певною конфігурацією кінцевої точки для віддаленої роботи. Навчання з питань безпеки в системи керування кінцевими точками є життєво важливими для надійної віддаленої кібербезпеки для організацій.

Чому навчання працівників кібербезпеці є важливим?

Коли мова заходить про кібербезпеку, організації повинні застосовувати проактивний підхід. Політика повинна базуватися на сценарії, що зловмисники отримають контроль над клієнтськими пристроями дистанційної роботи та спробують відновити з них конфіденційні дані або використовувати пристрої для отримання доступу до корпоративної мережі.

Згідно з даними дослідження CIS (Center for Internet Security):

- 95% проблем із кібербезпекою спричинені помилками людини.
- Кожні 39 секунд відбувається хакерська атака.
- У 2023 році середня глобальна вартість витоку даних склала 4,45 мільйона доларів.

Як навчити співробітників громадських та благодійних організацій кібербезпеці: 10 порад

Щоб звести до мінімуму ризик вторгнення в мережу, необхідно зміцнити свою першу лінію захисту від зовнішніх загроз — а це навчання ваших співробітників найкращим практикам кібербезпеки.

Поради щодо того, як навчити співробітників кібербезпеці.

1. Розробіть політику кібербезпеки вашої організації

Важко змусити ваших співробітників дотримуватися правил, якщо вони не знають, що вони є.

2. Допоможіть своїм співробітникам зрозуміти, що таке кібербезпека і чому це важливо саме в вашій організації

Наступним кроком до ознайомлення працівників з освітою з кібербезпеки є окреслення чіткого повідомлення про політику кібербезпеки вашої організації, обговорення конкретних ризиків та кейсів а також сценаріїв реагування.

Зрозумілість – використовуйте спрощені терміни, доступні нефахівцям.

Відповідність - Говорячи про зовнішні загрози, не варто говорити про центральну мережу, а більше про безпеку персонального комп’ютера та вторгнення в домашню мережу. Таким чином, працівники можуть особисто віднестись до небезпеки, якщо вона представлена в визначеннях їхнього телефону чи ноутбука. Це дозволяє їм мати особисту зацікавленість у плані безпеки: ніхто не хоче бути причиною витоку даних, що впливає на всю організацію.

Диверсифікованість – простого електронного листа з описом правил та рекомендацій може бути недостатньо. Подумайте, скільки електронних листів отримує окремий співробітник, як часто. Урізноманітнивши свою комунікаційну стратегію, ви зможете переконатися, що співробітники прочитають повідомлення, а не відкинуть його як спам.

3. Зробіть протоколи зрозумілими та пріоритетними для впровадження

У разі інциденту працівникам важливо знати правильний протокол. Це має включати певні зрозумілі кроки, обов'язкові для виконання. Це можуть бути такі кроки як повідомлення про будь-яку підозрілу активність, регулярна зміна паролів і підтримка програмного забезпечення в оновленому стані. Переконайтеся, що ці протоколи чітко доведені до відома всіх ваших співробітників.

Окрім зовнішніх загроз, навчання працівників щодо внутрішніх загроз має вирішальне значення. Це включає такі дії, як обмін конфіденційною інформацією з неавторизованими особами або використання корпоративних пристроїв для особистого використання. Створивши в компанії культуру обізнаності про безпеку, співробітники з більшою ймовірністю будуть повідомляти про будь-яку підозрілу поведінку своїх колег або щодо самих себе.

4. Забезпечте регулярне кібернавчання

Усі співробітники повинні пройти навчання з кібербезпеки під час вступу на роботу, але регулярне навчання також є важливим для всіх працівників. Навчання з кібербезпеки має охоплювати потенційні загрози та способи їх запобігання. Це може включати фішинг, тактику соціальної інженерії та захист від зловмисного програмного забезпечення. Також важливо мати призначену особу, яка може впоратися з будь-якими інцидентами безпеки, які можуть виникнути.

5. Заохочуйте дбайливо ставитися до своїх пристроїв

Згідно опитування Forrester показало, що 15% порушень корпоративних прав викликані втраченими або відсутніми пристроями. Незалежно від того, чи це корпоративний чи особистий пристрій, навчання ваших співробітників кібербезпеці включає в себе усвідомлення того, що їхній гаджет діє як шлюз до мережі вашої організації. Тому важливо доглядати за власним пристроєм і правильно ним користуватися, навіть у межах свого дому.

Допоможіть своїм співробітникам збільшити належне володіння пристроєм, виконавши такі дії:

- Поясніть різницю між особистим і корпоративним використанням власного та робочого пристрою.
- Зробіть обов'язковим наявність робочого облікового запису, який підлягає моніторингу, обмеженим встановленням і веб-фільтрації.
- Заплануйте час і надішліть інструкції як налаштувати безпекові параметри під особливості своєї діяльності.
- Обговоріть обмеження на встановлення нових додатків та доцільність використання певних додатків.
- Переконайтеся, що встановлено патчі безпеки та оновлення ОС.

Рішення для керування пристроєм і моніторингу, віддалене керування пристроєм із кількома ОС, може допомогти знизити ризик шляхом автоматизації push-оновлень і постійного відстеження стану пристрою та його місцезнаходження. Але це має служити

лише резервним копіюванням, а найкращі методи безпеки для кінцевих користувачів повинні залишатися за працівником.

6. Навчіть співробітників, як виявляти підозрілу діяльність

Покращуйте знання та навички своїх співробітників у виявленні підозрілих дій. Серед таких ознак можуть бути:

- Раптова поява нових додатків або програм на їхніх пристроях.
- Дивні спливаючі вікна під час запуску, нормальної роботи або перед завершенням роботи.
- Пристрій гальмує.
- Нові розширення або вкладки в браузері.
- Втрата контролю над мишею або клавіатурою.

Заохочуйте своїх співробітників негайно повідомляти про підозрілі ознаки. Навіть якщо це виявилося помилковою тривогою, це все одно може бути корисним для працівника, усунувши помилки в його пристрої, які заважають продуктивності.

7. Посилити конфіденційність

Робота вдома, як правило, робить людей більш самовдоволеними, що поширюється на кібербезпеку. Розкажіть про важливість паролів і автентифікації, навіть якщо вони працюютьу себе в кімнаті. Те, що вони розслаблені і у комфортній обстановці, не означає, що загроз не існує. Щоб уникнути загроз кібербезпеки щодо конфіденційності, навчіть своїх працівників виконувати наступні дії:

- Регулярно змінюйте унікальні паролі, використовувати менеджер паролів.
- Розкажіть співробітникам про небезпеку використання універсальних паролів і використовуйте реальні приклади минулих витоків даних, завітайте на ресурс перевірки паролів та як швидко його можна зламати зловмисникам.

  посилання на ресурси:

  https://nordpass.com/password-generator/

  https://bitwarden.com/password-generator/

- Обговоріть обґрунтування VPN, багатофакторної автентифікації та інших безпечних процесів входу в систему та чому вони важливі.
- Щоб боротися з незахищеним зберіганням даних компанії, наведіть конкретні приклади випадків викрадення даних, спричинених помилковим флеш-накопичувачем або скомпрометованим особистим обліковим записом.

  запропонуйте перевірити свій мейл на ресурсі:

  https://haveibeenpwned.com/

8. Вивчіть окремі випадки порушень кібербезпеки

На відміну від офісного середовища з контрольованою мережею, безпека домашніх комп'ютерів ваших співробітників може значно відрізнятися. Деякі можуть під'єднуватися через домашню мережу Wi-Fi, а інші можуть використовувати підключення через загальнодоступну мережу Wi-Fi у кав'ярні. Деякі можуть мати старіші пристрої, які більше не підтримуються виправленнями безпеки:

- Найкращий варіант коли співробітник використовує надані компанією пристрої.
- Проведіть перевірку безпеки домашніх мереж. Наприклад, деякі старі маршрутизатори можуть мати слабші протоколи WEP замість WPA-2, або деякі навіть можуть мати пароль за замовчуванням!
- Зверніть увагу на співробітників, які мають часткову зайнятість або залучені короткостроково або працюють з закордону і розробіть для них політику безпеки, оскільки дані в роумінгу або публічні точки доступу Wi-Fi несуть свої унікальні загрози.

9. Обов'язкове резервне копіювання важливих даних

Підкресліть, що дані належать компанії та повинні регулярно створюватися резервні копії, щоб запобігти втраті в разі збою пристрою або кібератаки. Заохочуйте співробітників використовувати надані компанією хмарні рішення для зберігання даних або зовнішні жорсткі диски для резервного копіювання — ніколи не їхні особисті пристрої — і нагадуйте їм робити резервні копії своєї роботи в кінці кожного дня, особливо якщо вони внесли значні зміни або доповнення.

Ось кілька порад, про які варто пам'ятати:

- Регулярне резервне копіювання є важливою частиною підтримки належної практики кібербезпеки.
- Надайте інформацію про те, як налаштувати автоматичне резервне копіювання за допомогою програм або вбудованих функцій пристроїв. Це може допомогти забезпечити постійне резервне копіювання важливих даних без ручного втручання співробітників.
- Заохочуйте співробітників періодично перевіряти свої файли резервних копій, щоб переконатися, що вони неушкоджені та придатні для використання в разі кібератаки.

10. Зробіть обізнаність про кібербезпеку постійною розмовою під час робочих нарад

У середньому співробітники витрачають до чверті свого робочого дня на завдання, пов'язані з електронною поштою. Це робить одноразове повідомлення електронної пошти про кібербезпеку невдалим вибором.

Ось кілька порад, якими можна скористатися, викладаючи повідомлення про кібербезпеку своїм співробітникам:

- Використовуйте різні підходи до навчання кібербезпеці.

- Для кожного оновлення дотримуйтеся правила KISS «Keep it short and simple» («Будь простіше і коротше»).
- Слідкуйте за сучасними трендами. Якщо є новий тип крипто-зловмисного програмного забезпечення або експлойту, який виводить з ладу телефони одним повідомленням, переконайтеся, що ваші співробітники знають про це.
- Щоразу використовуйте тактику привертання уваги, щоб змусити їх зрозуміти повідомлення. Замість того, щоб перераховувати суху статистику або що можна і чого не робити, спробуйте інфографіку. Для складних тем спробуйте відео пояснення.
- Використовуйте тести та симуляції

Системне навчання співробітників дозволить їм зрозуміти, яку роль вони відіграють у захисті організації. Замість того, щоб бути просто ще одним гвинтиком в організації, вони є першими очима, які захищають від зовнішніх загроз.

Ефективне інформування про кібербезпеку покладається на чітку комунікацію та безперервну освіту для надійного захисту від нових викликів безпеці.

***Підписуйтесь** далі поговоримо про те:*

- *як забезпечити безпеку мобільних присторіїв які стали звичним інструментом в робочих процесах*
- *та з чого почати впровадження безпекових політик в організації так щоб це був не просто формальний документ а дієвий інструмент.*

***Звертайтеся до нас за експертними порадами, розробкою політик безпекових навчань та аудитів.** Наші спеціалісти готові допомогти вам забезпечити безпеку вашої організації, підвищити ефективність роботи та допомогу громаді та спільнотам які потребують підтримки.*
