Асоціація Благодійників України

Ольга Гужва, експертка з кібербезпеки 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 експертної мережі DCN Global, Knowbe4 (USA)
guzhva(at)mediaexpert.group

“Пріоритетність кібербезпеки має вирішальне значення для неприбуткових та благодійних організацій, щоб захистити конфіденційну донорську інформацію, персональні данні бенефіціарів послуг, фінансові активи, зберегти довіру та підтримку у суспільстві, необхідні для виконання своєї місії. Впровадження дієвих політик та протоколів безпеки може допомогти зменшити загрозу кібератак, підвищити кіберстійкість організації, перевести знання співробітників про кібербезпеку в площину реальних поведінкових змін що підвищить рівень виявлення шахрайства та буде сприяти захисту критично важливих даних організації в цілому.”

Кібербезпека як пріоритет для неприбуткових організацій
Швидкий розвиток технологій відкриває нові можливості у використанні інформаційного простору, але також приносить нові загрози, особливо для громадських організацій, благодійних установ, активістів та волонтерів, які займаються зборами.

Ключові тенденції, які впливають на неприбутковий сектор у 2025 році
У 2025 році неприбуткові громадські організації мають великі можливості завдяки швидкому розвитку технологій, але це також приносить виклики та ризики. Неприбуткові організації, які покликані задовольняти життєво важливі потреби громади, часто залишають поза увагою заходи з формування та постійного підвищення кіберстійкості.

Відповідно до огляду останніх галузевих досліджень, можна виділити три ключові тенденції, які будуть все більше впливати на діяльність громадських організацій у 2025 році:

1. **Ширше використання штучного інтелекту (ШІ):** ШІ пропонує значний потенціал, та все більше громадських організацій впроваджують його у свою діяльність, оптимізуючи певні процеси, але це також створює нові ризики та виклики які треба усвідомлювати та знати.

2. **Збільшення впровадження електронних методів оплати:** Ці методи спрощують транзакції, але вимагають надійних заходів безпеки та обізнаність щодо методів шахрайства.
3. **Зростаюча увага кіберзлочинців та шахраїв:** Неприбуткові організації та окремі волонтери стають привабливими цілями через великі бюджети, якими вони оперують, і їхню публічну активність.

Розуміння цих тенденцій допоможе неприбутковим організаціям підвищити свою стійкість та значимість. Проактивно реагуючи на ці тенденції, неприбуткові організації можуть захистити свою діяльність та посилити свій ефективність своєї роботи у громадах.

Кіберзлочинність та кібербезпека: нові глобальні гравці
Представники благодійних організацій та фондів, громадські організації та волонтери, які займаються зборами, є привабливими цілями для кіберзлочинців через великі бюджети та публічну активність, також і тому що вони є “легкою наживкою” для шахрайства, бо досить часто не застосовують навіть базові знання з кібербезпеки на практиці.

- **Зростання кількості кібератак:** Згідно з звітом SonicWall (USA), загальна кількість кібератак зросла на 2% у 2023 році, зафіксовано близько 5,5 млрд епізодів.
- **Глобальні ризики:** Всесвітній економічний форум включив кіберзлочинність до топ-10 найсерйозніших глобальних ризиків наступного десятиліття (8 місце).
- **Зростання ринку:** Відповідно до дослідницького звіту Polaris Market Research, світовий ринок кібербезпеки був оцінений у 217,65 мільярдів доларів США у 2021 році та, як очікується, досягне 504,46 мільярдів доларів США до 2030 року, зростаючи на 9,7% протягом прогнозованого періоду.
- **Збільшення кількості інцидентів:** За даними FBI, кількість кіберінцидентів зросла на 400% у 2024 році, і ця тенденція продовжиться.
- **CERT-UA**, яка діє при Держспецзв’язку, в 2024 році опрацювала 4315 кіберінцидентів, повідомляє пресслужба відомства. Це на 69,8% більше, ніж у 2023-му.
- **Плани захисту веб-сайтів:** лише 68% неприбуткових організацій мають план захисту своїх веб-сайтів.
- **SSL сертифікати:** 84% встановили SSL сертифікати на своїх веб-сайтах, що на 14 пунктів більше, ніж у 2019 році.
- **Збільшення уваги до безпеки:** Згідно з опитуванням **AvidXchange 2025 Trends Survey,** безпека, шахрайство та спроби фішингу є головними проблемами для більшості неприбуткових організацій.

Потреба в знаннях та навичках з кібербезпеки

У 2022 році з'явилося 4300 нових унікальних назв посад у галузі кібербезпеки, і їх кількість буде зростати.

Неприбуткові організації часто називають "кібербідними" та "привабливими мішенямии",(“cyber-poor” and “target-rich,”) оскільки вони керують великими сумами грошей, але не вживають належних заходів кібербезпеки через обмежені бюджети та ресурси, а досить часто і через відсутність відповідних знань та фахівців.

Проактивне вирішення викликів кібербезпеки може допомогти неприбутковим організаціям захистити свою діяльність та посилити свій вплив. Розуміючи ризики та впроваджуючи ефективні заходи, вони можуть забезпечити безпеку своїх операцій, дозволяючи продовжувати ефективно допомогати громаді.

Архітектура нульової довіри для неприбуткових організацій

Що таке архітектура нульової довіри?

Архітектура нульової довіри (Zero Trust) – це сучасний підхід до кібербезпеки, який передбачає, що довіряти не можна нікому за умовчанням. Доступ до ресурсів надається лише після перевірки користувача і лише тією мірою, яка необхідна для виконання конкретного завдання.

Згідно із Національним інститутом стандартів та технологій (NIST, США), побудову архітектури нульової довіри можна здійснити кількома способами:

- **Привілеї доступу та верифікація користувачів на основі контексту:** Користувачі отримують доступ лише після підтвердження їхньої особи та врахування контексту запиту.
- **Сегментація мережі:** Мережа поділяється на окремі сегменти, захищені різними політиками та правилами доступу.
- **Програмно-визначувані підходи:** Використання програмно-визначуваних підходів до периметру для забезпечення безпеки.

Парадигма нульової довіри

Нульова довіра визнає, що довіра – це вразливість. Заснована на принципі **"ніколи не довіряй, завжди перевіряй"**, ця модель розроблена для захисту сучасних цифрових середовищ.
Термін "нульова довіра" вперше був використаний експертами Forrester, зокрема, Джоном Кіндервагом, для опису нової моделі безпеки, в якій користувачі та пристрої більше не поділяються на довірені та ненадійні групи. **Основна ідея цієї моделі – надавати доступ лише аутентифікованим та верифікованим користувачам.**

Інтерпретації моделі нульової довіри

У 2018 році експерти з кібербезпеки з Idaptive визначили нульову довіру як модель, що базується на триетапному процесі:

- Підтвердити особу користувача;
- Перевірити пристрій;
- Обмежити привілейований доступ.

У 2019 році Microsoft оголосила про впровадження моделі нульової довіри, зазначивши наступні кроки для створення ідеального середовища:

- Підтвердити особу користувача за допомогою аутентифікації;
- Перевірити працездатність пристрою за допомогою системи керування пристроями;
- Застосувати принцип найменших привілеїв;
- Перевірити працездатність використовуваних сервісів.

Збільшення бюджетів на кібербезпеку

За звітами KCAnalitic, організації збільшують бюджети на кібербезпеку. Це свідчить про усвідомлення важливості захисту даних та необхідності впровадження моделей, таких як нульова довіра.

Висновки та поради для громадських та благодійних організацій

1. **Розробка та впровадження стратегії кібербезпеки:** Необхідно регулярно оновлювати політики та процедури кібербезпеки. А якщо організація їх не має то спрямувати ресурси та час на їх розробку та впровадження.
2. **Навчання персоналу та волонтерів:** Проводьте тренінги з обізнаності про кібербезпеку та вчить як впровадити знання у практики.
3. **Інвестування в інструменти кібербезпеки:** Виділяйте ресурси на інструменти та технології кібербезпеки, такі як менеджер паролів, антивірусне програмне забезпечення та шифрування.
4. **Проведення регулярних аудитів безпеки:** Оцінюйте кібербезпеку організації та визначайте зони для покращення.
5. **Формування культури кібербезпеки:** Створюйте культуру в організації, яка базується на принципах нульової довіри, забезпечуючи відповідальність за безпеку на всіх рівнях.
6. **Співпраця з експертами:** Залучайте професіоналів з кібербезпеки для надання консультацій та підтримки.

Проактивний підхід до кібербезпеки допоможе неприбутковим організаціям захистити свої дані та посилити свій вплив у громадах. Впровадження архітектури нульової довіри забезпечить надійний захист та допоможе уникнути витоку даних.

Впровадження штучного інтелекту та електронних платежів у неприбуткових організаціях

- **Зростання впровадження штучного інтелекту**

Неприбуткові організації все частіше звертаються до штучного інтелекту (ШІ) для оптимізації адміністративної роботи та фандрейзингу. За даними опитування 2024 року, які **OneCause** висвітлила у своєму звіті **«Перспективи фандрейзингу у 2025 році»**, це свідчить про наступне:

- **49% організацій** використовують або планують використовувати ШІ для управління проєктами, що на 15 пунктів більше, ніж у 2023 році.
- **71% неприбуткових організацій** використовують або планують використовувати ШІ для копірайтингу, що на 19 пунктів більше, ніж у 2023 році.
- **71% некомерційних організацій** використовують або планують використовувати ШІ для фандрейзингу та планування заходів, що на 28 пунктів більше, ніж у 2023 році.

Дослідження тенденцій 2025 року, проведене **AvidXchange**, показало, що більшість організацій (65%) також використовують ШІ у своїх фінансових відділах. Хоча 76% опитаних фінансових керівників кажуть, що бачать користь у використанні ШІ для фінансових функцій, 71% зазначили, що стурбовані тим, як виміряти цей вплив.
У 2025 році організації, включаючи неприбуткові, продовжать надавати пріоритет технологічним інструментам, які використовують ШІ. Щоб забезпечити максимальну віддачу від цих інвестицій, вони, ймовірно, запропонують більше можливостей для навчання співробітників. Дослідження **AvidXchange** «Тенденції 2025» показало, що 65% організацій наразі проводять навчання персоналу з питань штучного інтелекту, а 50% пропонують можливості для підвищення кваліфікації та перекваліфікації, пов'язані з технологіями штучного інтелекту.

- **Зростання популярності електронних платежів**

Дослідження FundraiseUp виявило, що кредитні картки є найпопулярнішою формою оплати пожертв - 65% донорів надають перевагу цьому методу. FundraiseUp також виявив, що інші методи електронних платежів набирають обертів, і донори використовують такі платформи, як **PayPal (25%), Apple Pay (6%) і Google Pay (3%)** для здійснення благодійних пожертв.

Нещодавнє дослідження **UConn Busine**ss показало, що **пожертви онлайн зросли на 42% з 2019 року,** а **мобільні пожертви через смартфони склали 28% пожертв у 2021** році. Оскільки люди проводять більше часу на мобільних пристроях, неприбутковим організаціям найкраще інтегрувати методи електронних платежів у всі кампанії зі збору пожертв.

Організації, включаючи неприбуткові, також все частіше впроваджують електронні платежі у своїх фінансових операціях, користуючись перевагами зручності та підвищеної безпеки порівняно з іншими операціями. Опитування **AvidXchange «Тенденції 2025»** показало, що більшість організацій (61%) або виключно, або переважно використовують електронні платежі для розрахунків з постачальниками. Використання мобільних платіжних платформ (таких як Venmo та Apple Pay) для розрахунків з постачальниками також зростає, майже подвоївшись з 8% у 2023 році до 15% у 2024 році.

- **Переваги електронних платежів**

Електронні платежі можуть забезпечити більшу ефективність, безпеку та прозорість порівняно з паперовими варіантами, дозволяючи швидше обробляти платежі, зменшуючи ручну роботу та знижуючи ризик шахрайства або втрачених платежів.

Висновки та рекомендації

1. **Інвестування в штучний інтелект:** Неприбуткові організації повинні продовжувати впроваджувати ШІ для підвищення ефективності управління проєктами, копірайтингу, фандрейзингу та інших адміністративних функцій. Але при цьому усвідомлено працювати з ризиками та вразливостями.
2. **Навчання персоналу:** Забезпечити навчання співробітників щодо використання ШІ та нових технологій та розуміння ризиків та вразливостей.
3. **Інтеграція електронних платежів:** Впровадити методи електронних платежів у всі кампанії зі збору пожертв і фінансові процеси для підвищення зручності, безпеки та прозорості.
4. **Вимірювання рентабельності інвестицій:** Встановити чіткі метрики для вимірювання рентабельності інвестицій у ШІ та технологічні інструменти, щоб забезпечити ефективне використання ресурсів у звітній документації перед донором. Це дозволяє ор
5. ганізаціям зосередитись на своїй основній місії, зменшуючи витрати та підвищуючи довіру донорів.
6. **Кібербезпека:** Розробляйте та впроваджуйте стратегії кібербезпеки, проводьте регулярні аудити безпеки та формуйте культуру кібербезпеки в організації

Проактивне впровадження цих тенденцій та рекомендацій допоможе неприбутковим організаціям підвищити свою ефективність, безпеку та вплив на громади, яким вони допомогають. Однак ці зміни вимагають ретельного планування, навчання персоналу та впровадження відповідних політик кібербезпеки.

Прості кроки для ГО підвищити свою кіберстійкість:

Різке зростання кіберзагроз показує, що уникнути атак неможливо. Однак є дії, які можна вжити:

1. **Увімкніть багатофакторну автентифікацію (MFA):** Увімкнення MFA значно підвищує безпеку автентифікації. Навіть якщо хтось отримає доступ до ваших паролів, він не зможе отримати доступ до ваших облікових записів, оскільки для входу потрібна друга автентифікація від користувача.
2. **Оновлюйте патчі своєчасно:** Хоча про вразливості нульового дня існують, більшість атак намагаються скористатися вразливостями, яким вже кілька місяців або років.
3. **Проводьте регулярні оцінки безпеки:** Це допоможе вам виявити вразливості, оцінити ризики та проактивно зміцнити захист, забезпечуючи надійний захист від нових загроз.
4. **Проводьте постійні тренінги з безпеки:** З розвитком технологій розвивається і кібербезпека. Проводьте базові тренінги та рутинні практики - такі як заохочення співробітників не натискати на шкідливі посилання та навчання співробітників виявляти та повідомляти про потенційні загрози безпеці - щоб створити більш освічений та уважний колектив.
5. **Скануйте зашифрований трафік:** Експерти оцінюють, що сьогодні 80-90% усіх мережевих трафіків зашифровано. Однак багато застарілих брандмауерів не можуть виявляти, перевіряти та пом'якшувати кіберзагрози, передані через HTTPS-трафік. Згідно з даними SonicWall, з 2022 по 2023 рік кількість шкідливих програм, надісланих через HTTPS, зросла на 117%. Це підкреслює необхідність перевірки всього цього трафіку.
6. **Захистіть свій хмарний простір:** По мірі переміщення компаній даних і робочих процесів у хмару, необхідні більш комплексні та гнучкі підходи, включаючи Security Service Edge (SSE) та Zero-Trust Network Architecture (ZTNA) для гібридних робочих середовищ.

Зростання кіберзагроз у 2025 році: що нам готує майбутнє?

Кіберзагрози продовжують стрімко зростати, і дані за 2024 рік показують це чіткіше ніж будь-коли. За останній рік кількість шкідливих програм збільшилася на **30%**. Це вражаюче зростання підкреслює постійну еволюцію кіберзлочинців і їхніх методів.

Особливе занепокоєння викликає значне збільшення кількості шкідливих програм для Інтернету речей (**Internet of Thing або IoT** — концепція, яка передбачає об'єднання різних фізичних пристроїв через інтернет, дозволяючи їм взаємодіяти та обмінюватися даними.) - на **107%.** Це означає, що пристрої IoT стають все більш привабливою мішенню для хакерів. Оскільки ці пристрої все частіше використовуються в повсякденному житті, їхня безпека стає критично важливою для запобігання потенційним загрозам.

Зростання кіберзагроз для IoT: тривожні тенденції
У сучасному світі, де технології швидко розвиваються, Інтернет речей (IoT) стає все більш популярним. За даними **Statista,** у світі вже налічується понад 18 мільярдів розумних пристроїв, здатних передавати дані через Мережу. Однак, **дослідження Unit 42** показує, що 98% з них передають інформацію у незашифрованому вигляді! Це відкриває безліч можливостей для кіберзлочинців.

У першій половині 2023 року кількість кібератак на IoT досягла 77,9 мільйонів, що на 37% більше, ніж в аналогічний період 2022 року. Це вражаюче зростання підкреслює необхідність вдосконалення засобів захисту та підвищення кібербезпеки для IoT.

Ще одна тривожна статистика міститься у звіті **Keyfactor.** 97% організацій, що використовують смарт-пристрої у своїй роботі, стикалися з кібератаками. З цих організацій, 89% зазнали збитків через успішні злами, а 69% повідомляють про постійне збільшення тиску. Ці дані підкреслюють реальність загрози для кожного, хто використовує розумні пристрої у своїй роботі.

Основні висновки:

1. **Кількість розумних пристроїв:** Понад 18 мільярдів пристроїв по всьому світу.
2. **Незашифрований трафік:** 98% IoT-пристроїв передають дані у незашифрованому вигляді.
3. **Кібератаки на IoT:** У першій половині 2023 року кількість атак досягла 77,9 мільйонів (зростання на 37%).
4. **Вплив на організації:** 97% організацій стикалися з кібератаками, 89% зазнали збитків, 69% повідомляють про зростаючий тиск.

Рекомендації для підвищення кібербезпеки IoT:

1. **Використовуйте шифрування:** Забезпечте, щоб усі дані, що передаються через мережу, були зашифровані.
2. **Регулярно оновлюйте пристрої:** Забезпечте своєчасне оновлення прошивок і програмного забезпечення для виправлення вразливостей.
3. **Проводьте аудит безпеки:** Регулярно перевіряйте безпеку IoT-пристроїв і систем для виявлення потенційних загроз.
4. **Навчайте персонал:** Підвищуйте обізнаність працівників про загрози та методи їх запобігання.

У сучасному цифровому світі кібербезпека стає все більш критичною складовою успішної діяльності будь-якої організації. Однак, незважаючи на важливість, процес забезпечення кібербезпеки стикається з низкою викликів. Виявлення цих перешкод - перший крок до їх подолання та впровадження ефективних практик безпеки. Основні виклики включають:

1. **Людська помилка:** Людські помилки становлять значний виклик для кібербезпеки через потенційну можливість випадкового розкриття вразливостей або неправильного поводження з конфіденційною інформацією, що підвищує ризик витоків даних або несанкціонованого доступу.
2. **Неправильна конфігурація засобів безпеки:** Неправильна конфігурація засобів безпеки, особливо у хмарних середовищах, може призвести до критичних прогалин у захисних механізмах, залишаючи системи та мережі вразливими до кіберзагроз і несанкціонованого доступу.
3. **Блокування проти попередження:** Вибір між стратегіями блокування та попередження у кібербезпеці є важливим. Надмірна залежність від попереджень може призвести до незаблокованих загроз, тоді як надмірна кількість попереджень може перевантажити аналітиків, спричиняючи "втому від попереджень" та, можливо, упущення критичних інцидентів безпеки.
4. **Відкладене оновлення:** У багатьох випадках вразливості та подібні шкідливі програми були виявлені раніше, але програмне чи апаратне забезпечення залишаються незапатченими через затримку або відсутність оновлень. Це залишає пристрої вразливими для експлуатації навіть після того, як виправлення вже доступні.

5. **Типові конфігурації за замовчуванням:** Часто програмне та апаратне забезпечення не розроблені для оптимальної роботи "з коробки". Виділення часу на налаштування обладнання або пристрою може забезпечити вищий рівень безпеки.

Проактивні кроки для зміцнення вашої кібербезпеки

Сучасний ландшафт кіберзагроз розвивається неймовірно швидко, особливо з поширенням штучного інтелекту. Однак багато атак та загроз, можна уникнути, дотримуючись належних кібергігієнічних практик. Ось кілька проактивних кроків, які можуть значно зміцнити кібербезпеку громадських організацій:

1. **Пріоритезуйте швидке оновлення патчів:** Регулярне оновлення патчів є важливим, оскільки воно зменшує вразливості і знижує ризик дій зловмисників.
2. **Додайте багатофакторну автентифікацію (MFA):** MFA підвищує кібербезпеку, вимагаючи додаткових етапів верифікації, що значно зміцнює контроль доступу і запобігає несанкціонованим спробам входу.
3. **Посилення хмарної безпеки:** Оскільки організації досить активно переносять дані і операції в хмару, необхідно впроваджувати такі надійні заходи, як Security Service Edge (SSE) та архітектуру Zero-Trust Network (ZTNA), для захисту даних і додатків, забезпечуючи комплексний захист від кіберзагроз у хмарних середовищах.
4. **Безперервний моніторинг і реагування на інциденти:** Впровадження інструментів для реального часу виявлення загроз і розробка надійного плану реагування на інциденти можуть допомогти швидко зменшити і стримати кібернапади. Розгляньте різні можливість використання Центру операцій безпеки (SOC) та забезпечення цілодобового виявлення загроз для вашої організації.
5. **Сегментація мережі:** Поділіть мережі на менші, захищені сегменти, щоб обмежити вплив порушень і несанкціонованого доступу.
6. **Постійне навчання:** Постійне навчання з кібербезпеки є важливим для того, щоб співробітники були в курсі нових загроз, стратегій захисту та регуляторних вимог, що дозволяє швидко виявляти загрози і реагувати на них, запобігаючи витокам даних і фінансовим втратам. Це сприяє формуванню проактивної культури кібербезпеки, підвищуючи стійкість організації до нових загроз.

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.*

Підготовлено Ольгою Гужвою (https://vboabu.org.ua/)
