Ми прийшли в Бережу з різних напрямків інформаційної безпеки і тепер кожного дня робимо все від нас залежне, щоб використати наш попередній досвід для підвищення рівня захищеності наших клієнтів. За три роки з заснування “Бережа Сек’юріті” ми розробили власну методику перевірки захищеності організацій від загроз ***соціальної інженерії*** – методів впливу на людський фактор з метою компрометації конфіденційних даних та критичних бізнес-процесів.

Наша методика дозволяє здійснювати перевірку готовності організацій протидіяти атакам соціальних інженерів, виключає ризик неконтрольованих наслідків імітації таких атак, та забезпечує повний контроль над процесом тестування безпеки.

Здійснивши низку успішних випробувань нашої методики в реальних умовах, ми вирішили зробити наступний крок та сформувати нову унікальну пропозицію для організацій будь-якого масштабу та роду діяльності.

Протягом останніх років в кібер-безпеці спостерігаються дві чіткі тенденції: ***обсяг втрат організацій поступово збільшується***, ***а бюджет кібер-атак стрімко зменшується***. Популярне наразі кібер-шахрайство ***“CEO fraud”***, під час якого злочинці діють під виглядом керівників великих корпорацій, які вимагають терміново здійснити грошові перекази на рахунки нібито нових партнерів, коштувало світовій економіці ***два млрд. доларів у 2015 р***. при максимальній сумі втрат внаслідок одного інциденту ***понад 20 мільйонів*** та середній сумі ***близько 50 тисяч***. А банальний поштовий фішинг, внаслідок якого об’єкт атаки шахраїв сам відкриває Троянську програму або переходить за посиланням на зловмисний веб-сайт, що міститься в електронному листі, може коштувати корпорації-жертві ***до 3,7 мільйонів доларів***.

На тлі ескалації геополітичних конфліктів в різних частинах Світу ми спостерігаємо поступове розширення списку країн, які створюють та збільшують свій наступальний потенціал в кібер-просторі. Якщо раніше ми були впевнені, що цілями кібер-атак на державному рівні можуть бути лише державні установи або тісно пов’язані з ними приватні компанії, то останнім часом ми є свідками перегляду цих правил гри в бік розширення переліку потенційних цілей спецслужб, який тепер включає ***об’єкти енергетики та транспорту, медійні компанії, громадські об’єднання та інші недержавні організації***.

З технологічної точки зору, здійснення успішної атаки з використанням соціальної інженерії ніколи не було чимось надскладним: якщо у нападника не було відповідного таланту, він завжди міг скористатися методами, докладно висвітленими у спеціальній літературі та мемуарах відомих соцінженерів.

Усі досвідчені спеціалісти з безпеки чудово знають, що ***вразливості зазвичай виникають на стику технологій***: там де одне технологічне рішення вступає у взаємодію з іншим. І при цьому ризик виникнення проблем безпеки тим вищий, чим суттєвіша різниця між технологіями, що взаємодіють. За таких умов ніщо не може бути більш ризикованим за ***взаємодію високих технологій та людської істоти***.

Ситуація ускладняється тим, що внаслідок різкого зросту доступності Інтернету та популярності соціальних медіа, інформація щодо цілей атак соціальної інженерії – працівників компаній – стала ще більш доступною та детальною. А пошук та систематизація такої інформації легко автоматизується програмними інструментами, які зазвичай поширюються безкоштовно або за помірну платню.

За таких умов ми не можемо розраховувати, що найближчим часом загроза здійснення кібер-атак з використанням соціальної інженерії буде скорочуватись. У той час, коли індустрія кібер-безпеки відчайдушно намагається протидіяти загрозам експлуатації людського фактору технологічними методами (вартість яких в змозі дозволити собі лише найприбутковіші світові корпорації), ми усвідомлюємо, що універсальність вразливостей людської поведінки вимагає створення такого ж універсального методу захисту, зрозумілого кожному користувачу.

Для організацій, які усвідомлюють критичність кібер-безпеки для їхнього бізнесу, і які незадоволені сучасним станом пропозиції на ринку засобів захисту, ми розробили нову категорію послуг з підвищення рівня кібер-безпеки шляхом ***укріплення найслабшої ланки системи захисту – людського фактору*** – та перетворення її у потужний та економічно ефективний інструмент безпеки.

На відміну від технічних засобів безпеки, що відзначаються обмеженою ефективністю, особливо, коли йдеться про протидію загрозам соціальної інженерії, розроблений нами комплекс послуг дозволяє озброїти організації дієвими засобами захисту та об'єктивно перевірити їх ефективність.

Наша пропозиція складається з таких кроків:

1. ***Первинна перевірка*** захищеності організації від кібер-атак з використанням соціальної інженерії;
2. ***Проведення одноденного авторського тренінгу*** з протидії загрозам соціальної інженерії;
3. ***Повторна перевірка*** захищеності.

Підчас перевірки ми використовуємо власну методику виконання тестів на проникнення по соціальному каналу, яка забезпечує повну контрольованість дій команди тестування та виключає ймовірність непередбачуваних наслідків.

У ході навчання ми використовуємо ***унікальну програму*** підвищення обізнаності персоналу з питань протидії соціальній інженерії, яка створена на основі найбагатшого в Україні досвіду з проведення тестів на проникнення по соціальному каналу та результатах здобутків світової науки в області ***прикладної психології, нейрології, теорії ігор та поведінкової економіки***.

Програма навчання налаштовується ***індивідуально для кожної організації*** та категорії слухачів та включає чотири основні розділи:

- ***Типи*** сучасних кібер-атак, ***методи*** їх здійснення та ***виконавці***;
- ***Категорії кібер-атак***, які використовують елементи ***соціальної інженерії***, способи їх виявлення та протидії ним;
- Принципи та ***методи впливу*** на рішення та поведінку людей, способи протидії методам впливу з мінімальними наслідками для цілі;
- ***Універсальний метод протидії атакам соціальної інженерії***.

На основі нашого досвіду та результатів передових наукових досліджень, ми розробили ***метод протидії соціальній інженерії***, який дозволяє ефективно протистояти сучасним кібер-атакам у ***три прості кроки***. Тепер ми пропонуємо вам скористатися ним з метою дієвого та ефективного захисту від найскладніших кібер-атак та традиційного кібер-шахрайства.

Бажаєте дізнатися більше?
http://berezhasecurity.com
sales@berezhasecurity.com
PGP: 82C6 8DBF DF4B 8DF5