Деякі організаційно-психологічні напрямки забезпечення кібербезпеки у державі.

Косиченко О.О.
доцент кафедри економічної та інформаційної безпеки
Дніпропетровського державного університету
внутрішніх справ, кандидат технічних наук.

Останнім часом ми часто зустрічаємося із подвійним відношенням до питання інформаційної безпеки. З одного боку, хвилі надмірної паніки, відчутні після великих кібератак, з іншого боку - надмірно легковажне відношення. Дані різних опитувань, проведених в останні роки, як правило, указують на низьку культуру безпеки в організаціях. Мова при цьому йде тільки про технічні заходи захисту інформації, як про малу увагу до освіти. І це незважаючи на те, що ці ж дослідження акцентують увагу на тому, що деякі із самих вражаючих по масштабом кібератак відбулися саме в результаті недостатньої інформованості персоналу.

Так що те, наскільки серйозно та або інша компанія ставиться до корпоративної культури кібербезпеки, сильно відрізняється: співробітники однієї організації можуть проходити безліч тренінгів і одержувати всілякі вказівки, у той час як співробітники іншої фірми можуть знати, що в принципі правила кібербезпеки важливі, але вирішувати реальні проблеми вони будуть самостійно. Для керівників сьогодні важливе розуміння і основ, і питань, пов'язаних з конкретним використанням технологій. Але отут є складність: поняття "основи" постійно розширюється. Представникам бізнесу доводиться адаптуватися до постійно зростаючого списку технологій. Потрібно одночасно думати, наприклад, про захист девайсів від неавторизованого застосування та від атак шкідливих програм, про збереження систем у в робочому стані, про захист конфіденційної інформації, про захист персональних даних, про безпечне використання мереж, про безперебійне створення резервних копій даних на випадок втрати, крадіжки або поломки обладнання. Це аж ніяк не вичерпний список нових кіберзагроз. Причому кожна з погроз небезпечна одночасно для обладнань самого різного типу. Наприклад, ще кілька років назад віруси були реальною проблемою тільки для десктопів і ноутбуків. Зараз нам доводиться побоюватися їхнього проникнення в смартфони, планшети

та в інші гаджети. Багато із цих проблем стосуються не тільки корпоративних систем, але рядових користувачів. Багато з перелічених погроз спрямовані безпосередньо на приватних користувачів: фішинг, спрямований на одержання доступу до конфіденційної інформації; шкідливі програми, які цілком успішно використовують системи кінцевих користувачів як засіб відправлення спама або запуску атак проти інших мішеней, і так далі. Знання тих самих основ може допомогти забезпечити захист людини – і як індивідуального користувача, і як співробітника на робочому місці. Так що, поліпшуючи освіту у сфері безпеки та підвищуючи поінформованість про проблеми, ми вирішуємо кілька проблем. В інтересах кожної компанії мати персонал, який би сам міг забезпечувати свою безпеку. Тоді працівники будуть краще справлятися із захистом власних систем і даних.

Ключовий спосіб навчання персоналу – через зіткнення з погрозами, які можуть виникнути з найбільшою ймовірністю. Проте, навчити співробітників точно розпізнавати погрози різної природи неможливо. Інший підхід – переконатися, що співробітники знають, які об'єкти особливо коштовні та важливі, і усвідомлюють необхідність їх захисту. У деяких організаціях мова може йти про документи, системи, дані — для них використовують інформаційні класифікації начебто "конфіденційно" або "секретно". Маркування вказують на необхідність працювати з такою інформацією особливим способом. Коли співробітники досить інформовані про цінність даних, з якими мають справу, вони куди частіше замислюються про свої дії, перш ніж ділитися доступом до даних.

Важко назвати основні погрози для компаній, не перераховуючи в остаточному підсумку той самий список потенційних проблем, з якого ми почали. Опитування звичайно називають найпоширенішими погрозами ті, що пов'язані зі шкідливими програмами, фішінговими повідомленнями, у цілому із проблемами, що випливають із необхідності для бізнесу працювати з зростаючим обсягом даних. Однак найбільш шкідливими та впливовими стають разові погрози, наприклад погрози з боку самого персоналу. Також важливо не випускати з уваги погрози, що виникають у результаті випадкових подій – збоїв систем, порушень у роботі обладнання. Адже збиток у таких випадках може бути настільки ж масштабним, як і у випадку цілеспрямованих атак зловмисників.

Кіберзагрози прийнято ділити на внутрішні й зовнішні. Найчастіше увага керівників компаній зосереджена на зовнішніх погрозах, – наприклад, на протидії атакам хакерів, на захисті від

шкідливих програм (такі атаки широко висвітлюються в ЗМІ). Проте навмисні погрози зсередини компанії – шахрайство, неавторизований доступ, крадіжка даних – не менш небезпечні. Вони можуть бути замасковані. До того ж деякі внутрішні погрози виникають у результаті ненавмисних дій або недостатньої поінформованості співробітників. Деяких з подібних ризиків можна уникнути саме за рахунок більш якісного навчання персоналу. Інша група ризиків, пов'язаних із внутрішніми погрозами, вимагає не стільки освіти співробітників, скільки налагоджених систем моніторингу, чітких алгоритмів виявлення інцидентів кібербезпеки.

Існує величезна необхідність навчання звичайних користувачів, інакше ми просто виявимося в ситуації повної уразливості всіх громадян. Якщо приватні користувачі не будуть знати, як себе захистити, вони ненавмисно можуть збільшити ситуацію й для себе, і для інших, у тому числі для бізнесу. Наприклад, якщо моє обладнання не захищене й заражається шкідливим програмним забезпеченням, а потім починає атакувати інші системи як частини "ботнету", це означає, що проблема вже не винятково моя. Недостатня безпека мого обладнання фактично впливає на інших.

Є базові правила, які повинні бути відомі всім. Їх можна розглядати як мінімально необхідний рівень знань у сфері кіберінформаційної грамотності. Молоді користувачі можуть одержати основні знання в рамках традиційної системи освіти. Для користувачів, які вже пройшли всі стадії освіти, методики навчання можуть варіюватися. Наприклад, у Великобританії працює портал *Get Safe Online (www.getsafeonline.org)*, він дає ради як приватним користувачам, так і представникам бізнесу. Сайтів такого рівня якості в Україні практично немає.

Держава повинна турбуватися про інформаційну безпеку, тому що проблеми в цій сфері впливають на схильність громадян злочинам різного виду. Держава повинна взяти на себе контролюючу роль: якщо кожний громадянин захищений, його поведінка не шкодить усім іншим. Гарна аналогія - контроль держави за безпекою на дорозі. Наявність правильних вказівок захищає не тільки окремого водія, але пішоходів та водіїв.