Олександр ТИТАРЕНКО
старший викладач кафедри інформаційних технологій
та інформаційних систем ДРІДУ НАДУ

ФОРМУВАННЯ КУЛЬТУРИ КІБЕРБЕЗПЕКИ В ОРГАНАХ ПУБЛІЧНОГО УПРАВЛІННЯ УКРАЇНИ

13 лютого 2017 року Президент України ввів у дію рішення Ради національної безпеки і оборони від 29 грудня 2016 року «Про загрози кібербезпеки держави та невідкладні заходи щодо їх нейтралізації» [1]. За підрахунками команди реагування на комп'ютерні надзвичайні події України CERT-UA в українському сегменті мережі Інтернет на поточний момент близько 2500 веб-сторінок, які презентують державний сектор України [3]. З них приблизно половина має ознаки компрометації і це тільки вершина айсбергу, адже про «кіберзло» відомо далеко не все.

Протягом листопада – грудня 2016 року близько 6,5 тис. спланованих кібератак були виявлені в Україні на об'єктах п'яти відомств і 31 державного інформаційного ресурсу. У першу чергу це – підприємства енергетичного сектора і державні структури. Ці кібератаки мали серйозні наслідки, незважаючи на те, що практично кожна з постраждалих організацій володіла засобами антивірусного захисту.

Загрози у кіберпросторі постійно змінюються. Традиційні загрози набувають більш небезпечних, підступних та ефективних в дії типів, наприклад Advanced Persistent Threats (APT) – просунуті стійкі загрози. CERT-UA регулярно фіксує атаки на органи державної влади України які мають усі ознаки APT. Найчастіше джерелами APT є установи, що фінансуються з державних бюджетів та мають цілі, що виходять далеко за межі простої крадіжки: військова розвідка, економічний саботаж, технічний шпіонаж, фінансові махінації, політичні маніпуляції.

У той час, коли органи публічного управління все більше переводять свою діяльність у цифровий світ і створюють нові канали взаємодії з користувачами, постійні мутації кіберзагроз породжують нові ризики і нові питання. Для органів управління сьогодні важливим є завдання визначення як використовувати проривні технології і тенденції, такі як Інтернет речей, хмарні технології, мобільні пристрої та контролювати ризики, що виникають в системах електронного урядування.

Керівники органів публічної влади все більше усвідомлюють необхідність забезпечення передових технологій кібербезпеки. Але щоб реагувати на інциденти тільки усвідомлення цього недостатньо ─ питання кібербезпеки повинні бути предметом постійної уваги. Та незважаючи на інформаційно-пропагандистську роботу, що проводиться засобами масової інформації, люди недостатньо комп'ютерно грамотні і досі не сприймають повною мірою загрози, не виконують необхідних дій з реалізації заходів кібербезпеки, не навчені культурі кібербезпеки.

Сьогодні можна з упевненістю говорити, що кожна людина була, є, або буде жертвою кібератаки. Цього майже неможливо уникнути. Особливої уваги потребують ризики, пов'язані з соціальною інженерією. Метод соціальної інженерії орієнтований не на інформаційну або технічну складову інформаційної системи, а на людину, як найбільш слабку ланку цієї взаємодії. Основне завдання цього методу – змусити користувача виконати дії, які необхідні зловмиснику для ураження його автоматизованого робочого місця. Саме цей метод ураження є сьогодні найбільш поширеним у інформаційному просторі. Публічні службовці нині повинні бути свідомі того, що вони самі є мішенню для фахівців соціальної інженерії і повинні бути спроможними самим захистити себе. Це, безсумнівно, вимагає обізнаності персоналу органів публічного управління з цього питання

Еволюція кіберзагроз відбувається також паралельно з надзвичайно швидким розвитком мобільних та соціальних технологій, поширенням смартфонів і інших мобільних гаджетів. І якщо політика BYOD (Bring Your Own Device – свобода вибору терміналу) здається менш актуальною на вищому рівні, на місцевому рівні органи публічного управління повинні керувати цим процесом, прививати культуру користування та здійснювати відповідні заходи із кібербезпеки. У цьому контексті культура мобільної кібербезпеки має формуватися, підтримуватися та бути пов'язаною з програмами підвищення кваліфікації і навчання користувачів, щоб залишатися на рівні реальних загроз.

Наслідки від кіберзлочинів стають все більш руйнівними і виконавчі та місцеві органи влади повинні дотримуватися усе більш жорстких та обов'язкових правил кібербезпеки. Рекомендації та засоби, що надає державна служба спецзв'язку та захисту інформації, значно збільшують навантаження задля їх дотримання і не всі організації мають необхідні ресурси для їх запровадження у повній мірі. Безпека та стійкість інформаційних систем стають завданнями не тільки для фахівців і груп забезпечення безпеки персоналу. Якщо ІТ-відділ відповідає за безпеку мережі, то запобігання вторгненням стає справою кожного. Кібербезпека стає колективною відповідальністю і всі публічні службовці повинні нести особисту відповідальність. Персонал повинен розуміти, що кібербезпека – це справа кожного, особливо якщо йдеться про сферу публічного управління. Такий розвиток подій неминуче вимагає формування в органах публічного управління України культури кібербезпеки і розгляду цієї проблематики у значно ширшому контексті.

Існує кілька сотень визначень поняття культури. За визначенням Р. Лінтона «культура ― це сукупність засвоєних форм поведінки і її результатів, елементи яких є загальними та передаються серед членів певного суспільства». У цьому контексті під культурою кібербезпеки в органах публічної влади розуміється розробка, засвоєння та додержання правил поведінки у віртуальному просторі які забезпечують безпечне функціонування публічних інформаційних систем та критичної інформації. Проблема кібербезпеки організації виходить далеко за рамки розгляду одного компонента, чи то захист даних, мобільних пристроїв або хмарних середовищ. Культура кібербезпеки

охоплює всі такі пов'язані елементи. Формування та підтримка культури кібербезпеки в органах публічної влади не тільки полегшує дотримання правил, але й забезпечує інші функції, зокрема безпечного обміну даними. Розвиток культури кібербезпеки має йти поряд з будь-якими новими підходами щодо кібербезпеки, бо жоден проект не може домогтися успіху без участі людського фактору. Основний інтерес культури кібербезпеки полягає в тому, щоб кожен службовець знав свої права та обов'язки і знав про свою індивідуальну відповідальність.

Невід'ємними елементами культури кібербезпеки мають бути парольна політика, відсутність на робочих комп'ютерах службовців додатків, сервісів та служб, які не є необхідними для виконання ними своїх службових обов'язків, вміння співробітників виявляти кібератаки, у разі їх проведення, наявність регулярно поновлювального плану реагування на інциденти в області кібербезпеки, описаний порядок дій користувачів у разі виявлення ознак порушення штатного режиму функціонування інформаційних систем.

Оскільки не всі установи районного, міського, сільського рівня мають досвідчених системних адміністраторів, або і зовсім їх не мають, елементом культури кібербезпеки співробітників має стати самостійне регулярне сканування автоматизованих робочих місць на предмет наявності шкідливого програмного забезпечення та регулярне оновлення антивірусного програмного забезпечення згідно з наказом Адміністрації Держспецзв'язку від 26.03.2007 р. № 45.

Керівники і співробітники органів державної влади та місцевого самоврядування повинні бути готові до інтеграції практики кібербезпеки у своє повсякденне життя – вимірювати ступінь уразливості своїх комунікацій і ризиків перехоплень за межами роботи, оцінювати стійкість своїх паролів, зважено підходити до своєї присутності у соціальних мережах, обережно підключатися до відкритих Wi-Fi мереж для передачі службових і конфіденційних даних.

Для співробітників органів публічного управління та користувачів публічних послуг безпека інформації має життєво важливе значення. Проте, якщо громадяни в першу чергу хвилюються за свої особисті дані, співробітники органів публічної влади повинні не тільки забезпечити абсолютну безпеку власного середовища, але й проявляти максимальну пильність щодо ризиків, пов'язаних із зовнішніми атаками. Через характер інформації, якою вони оперують, зазначені органи мають розуміти важливість підвищеної кібербезпеки своїх інформаційних систем та протистояти найрізноманітнішим атакам, від DDoS атак (розподілена відмова в обслуговуванні) до витоку даних. І зрозуміло, що усі ці загрози постійно розвиваються.

Культури кібербезпеки потрібно дотримуватися усім, у тому числі керівництву та IT-персоналу. Керівники частіше стають мішенню тому, що мають доступ до додаткової та більш конфіденційної інформації, ніж інші, вони часто є більш уразливими, коли знаходяться далеко від місця своєї роботи. Співробітники IT-відділу більш уразливі через свої привілейовані права доступу до всієї мережі організації.

Міцність ланцюга послідовних заходів кібербезпеки обмежується його найслабшою ланкою, а саме – персоналом. Необхідно свідомо визнати і донести до персоналу, що всі люди мають недоліки і роблять помилки, а співробітники є найбільш слабкою ланкою щодо кібербезпеки. Потрібно постійно проводити навчання службовців кібербезпеці ─ обізнаність персоналу є одним з пріоритетів створення культури кібербезпеки. Інтеграцію нових співробітників до програм кібербезпеки необхідно розпочинати з відділу кадрів. До вступу на посаду, перш ніж майбутні співробітники матимуть доступ до комп'ютерної техніки вони повинні знати основи кібербезпеки. Підтримуватися увага співробітників до питань кібербезпеки повинна до моменту їх звільнення.

Рекомендації парламентських слухань на тему «Реформи галузі інформаційно-комунікаційних технологій та розвиток інформаційного простору України», схвалені Постановою Верховної Ради України, рекомендують Міністерству освіти і науки України «розробити та впровадити програму підвищення обізнаності громадян з питань інформаційної безпеки, кібербезпеки та захисту інформації щодо захисту конфіденційної інформації, зокрема персональних даних, протидії загрозам її несанкціонованого використання» [2].

У прищеплені працівникам органів публічної влади культури кібербезпеки провідна роль належить Національній академії державного управління та її регіональним інститутам. Реалії віртуального світу вимагають доповнення на всіх формах навчання наявних поодиноких лекцій і короткострокових курсів з інформаційної безпеки освітніми програмами, заснованими на ключових стандартах кібербезпеки (ISO 27001, ISO 27002), кіберстійкості (Resilia) та управління комп'ютерними мережами для лідерів (COBIT). Відповідні розділи з розвитку культури кіберзахисту повинні містити і різноманітні програми інформатизації, у тому числі й регіональні.

Список використаних джерел

1. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації» : Указ Президента України від 13 лютого 2017 р. № 32/2017. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/32/2017.

2. Про Рекомендації парламентських слухань на тему: «Реформи галузі інформаційно-комунікаційних технологій та розвиток інформаційного простору України» : Постанова Верховної Ради України від 31.03.2016 р. № 1073-VIII. // Відомості Верховної Ради (ВВР), 2016, № 17, ст. 191. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/1073-19

3. Рекомендації від CERT-UA. – Режим доступу : http://cert.gov.ua/?page_id=535

4. Instaurer une culture de la cybersécurité au travail : Mode d'emploi − Access mode : https://www.globalsign.fr/fr/blog/instaurer-une-culture-de-cybersecurite-au-travail/#accept