# ДЕЯКІ АСПЕКТИ КІБЕРБЕЗПЕКИ В СФЕРІ БІЗНЕСУ: РЕКОМЕНДАЦІЇ ЩОДО СТАЛОГО РОЗВИТКУ ЕКОНОМІКИ

**М.Д. Василенко**
*Національний університет «Одеська юридична академія», професор кафедри господарського права і процесу, доктор юридичних наук, доктор фізико-математичних наук*

Кожна країна ставить перед собою ціль мати успішну економіку. В ліберальній економіці кожна країна намагається бути привабливою для споживачів, коли її дії спрямовані на отримання задоволення від володіння чи використання певного продукту та надихаються ідеями для створення чи підвищення рівня власних сервісів та стримуванні конкурентів і в зупиненні їх розвитку. Використання комп'ютерних технологій, особливо у сукупності з телекомунікаційними мережами, породило особливий (вірусний) клас кіберзагроз. Ситуація набувала загострення разом з поширенням використання мережі Інтернет, тобто існуючі кіберзагрози розв'язуються через забезпечення саме кібербезпеки та її постійного покращення. Проблема кібербезпеки гостро виявляється тоді, коли можлива реальна шкода у великих обсягах від реалізації загроз у сферах, де використовуються комп'ютерні системи та телекомунікаційні мережі. При цьому залишається важливим, що якість та безпечність продукції мають відповідати встановленим технічним стандартам. Однак в процесі реалізації ланцюга сировина-готовий продукт трапляється безліч фатальних помилок за які суб'єкти господарювання мають нести господарську відповідальність. Сьогодні багато компаній зазнають зовнішньої атаки або зіштовхувалися з внутрішніми інцидентами інформаційної безпеки при поширенні ринку вірусів. Сайти малого, але набираючого попиту проекту може цілком легко опинитися під випадковою DDoS-атакою. Не викликає сумнівів, що кібератаки сильніше і частіше зачіпають малий і середній бізнес, оскільки такі компанії помилково вважають себе «нецікавими» в плані інформаційних ресурсів, котрими володіють. При цьому лідерами за кількістю встановлених систем залишаються різні дис-

трибутиви Windows і Linux. Очевидно, що обслуговування машини на Linux є дешевшим через безкоштовність цієї системи, проте також слід відзначити і відкритий код Linux, що допомагає атакуючій стороні виявити недоліки і слабкі місця у системі захисту. Взагалі дистрибутив операційної системи, який встановлений на обслуговуючій машині об'єкта є одним із визначних чинників, що впливають на рівень кіберзахищенності структури. Останнім часом популярними стали атаки на веб-сервера саме через ssh протокол, який використовується для доступу до керування веб-сервера саме на системі Linux. Тобто такий вид кібератак – це фактично напад на сервер, на якому зберігаються стратегічно важливі дані, а також часто дані, котрі необхідні для координації веб-сайту або веб-сервісу об'єкта нападу. Особливою небезпекою таких атак є те, що вони майже повністю паралізують інформаційну інфраструктуру об'єкта нападу і збитки, спричинені такою кібератакою, відповідно, будуть глобальнішими.Найпоширенішим видом кіберзлочинів залишається кардинг, що представляє собою використання в операціях реквізитів платіжних карт, отриманих зі зламаних серверів інтернет-магазинів, платіжних і розрахункових систем, а також із персональних комп'ютерів (або безпосередньо, або через програми віддаленого доступу, «трояни», «боти»). «Фішинг» є видом шахрайства, відповідно до якого клієнтам платіжних систем надсилають повідомлення електронною поштою нібито від адміністрації або служби безпеки цієї системи з проханням вказати свої рахунки та паролі. Такий вид киберзлочинів як «вішинг» базується на тому, що в його повідомленнях міститься прохання зателефонувати на певний міський номер, а при розмові запитуються конфіденційні дані власника картки. Онлайн-шахрайство – це несправжні інтернет-аукціони, інтернет-магазини, сайти та телекомунікаційні засоби зв'язку.

Реально великої шкоди усім завдає «мальваре» – створення та розповсюдження вірусів і шкідливого програмного забезпечення. Все ж таки відзначимо два принципових види кібератак: спрямований фішинг (Spear Phishing) (перша лінія атаки) та «Watering Holes». У той час як традиційні фішинг-атаки розкинули широку мережу, розсилаючи електронні листи сотням або тисячам адресатів, спрямовані фішинг-атаки (гарпунний фішинг, Spear Phishing) націлені на невеликі підгрупи людей, як правило, співробітників

компаній. Шахрай, який планує спрямовану «фітинг»-атаку, може створити фальшивий електронну адресу співробітника і з нього написати кільком легітимним співробітникам, запитуючи інформацію про компанію. Думаючи, що вони спілкуються з колегою, легітимні співробітники можуть надати цю інформацію. І саме тут постає питання налаштування корпоративної пошти, а саме SPF цифрового підпису, значення якого і визначає сервера з яких можна надсилати пошту з корпоративного домену. Також важливим етапом захисту є перевірка технічного заголовку листа, в якому міститься інформація про час надсилання листа і поштові сервери. Тож постає питання інструктажу робочого персоналу щодо основних правил інформаційної безпеки. Проведення такого тренінгу для робочого персоналу не призведе до великих затрат, проте може попередити досить значні загрози.

У разі використання стратегії атаки типу «Watering Holes» хакери розміщують шкідливі програми в коді веб-сайтів, які з найбільшою ймовірністю відвідують співробітники компанії, що атакується. Якщо працівник заходить на такий сайт з комп'ютера компанії, вся мережа компанії може піддатися вірусу, що збиратиме дані.

Причина того, чому кібератакам піддається саме малий і середній бізнес досить проста. Великі організації, як правило, зберігають важливі дані на власних серверах, в той час як малі та середні орендують віддалені сервера.

Малому та середньому бізнесу необхідно стати більш захищеними, оскільки число шкідливих програм збільшується, і вони не розпізнаються. Коли кібератаки здійснюються опосередковано через «Watering Holes», немає меж, що визначають, що вірус буде поширюватися тільки на великі компанії. Тепер додамо той факт, що підприємства малого і середнього бізнесу мають менше захисних бар'єрів. Як результат: малі підприємства відчувають максимальну вагу таких кібератак.

Одна з найбільших переваг малого і середнього бізнесу – це здатність бути швидкими і мобільними. Команди таких підприємств іноді побоюються, що посилення безпеки означатиме втрату продуктивності, так як користувачі загрузнуть у процесах аутентифікації. Однак є кілька способів для досягнення безпеки від хакерів і втрати або крадіжки девайсів без встановлення великої кількості обмежень на діяльність працівників, а також без вагомих фінан-

сових затрат на забезпечення роботи такого механізму. Одним з прикладів таких способів захисту даних може виступати безперервне шифрування. Сьогодні можливо захистити дані, де б вони не зберігалися, – на мобільному чи пристрої або на настільному, в портативних чи медіа-сховищах або хмарі, – не ускладнюючи доступ для співробітників. З безперервним шифруванням, співробітники можуть мати доступ і обмінюватися даними, не витрачаючи час на надмірні заходи безпеки і не маючи справи з повільною завантаженням інформації.

Також інструментом захисту інформації може слугувати розширена аутентифікація, що об'єднує кілька форм аутентифікації для того, щоб переконатися в тому, що люди, які намагаються отримати доступ до даних компанії, є тими, ким вони представляються. Компанії можуть використовувати комбінацію апаратної аутентифікації, аутентифікації на основі облікового запису і шляхом цифрового підпису, щоб переконатися, що ніхто не отримає доступ до файлів, які їм не дозволено бачити.

Не слід нехтувати програмами стримування загроз. Сьогоднішні програми стримування шкідливих програм автоматично розпізнають і зупиняють шкідливі програми перш, ніж ті поширяться. Програми стримування загроз вказують браузерам запускати найбільш часті адресні програми у віртуальному середовищі. Таким чином, навіть якщо працівник відвідує сторінку, яка містить шкідливу програму, ця програма не може спрацювати і атакувати власника операційної системи. Крім того, ці системи можуть визначити шкідливі атаки, ґрунтуючись на поведінкових факторах, а не на підписах, тому компанія може зупинити поширення атак 0-day (zero-day загроза – zero-day; шкідливі програми, проти яких ще не розроблені захисні механізми). Слід заначити, що більша частина інструментів для захисту інформації є безкоштовними і водночас надійними. Тож робота кваліфікованого фахівця допоможе уникнути витрат на дороге програмне забезпечення.

Отже, визначено головні чинники кібербезпеки в економіці: механізм захисту серверу, який зберігає, координує і передає важливі дані компанії; наявність цінної інформації у розпорядженні компанії; обізнаність працюючого персоналу з питань інформаційної безпеки; використання інструментів розширеної аутентифікації, інструментів стримування поширення загроз тощо. Втілення зазна-

чених методів захисту інформації у роботі реальної економічної структури значно зменшить ризик стати жертвою кібератаки. Наголосимо на декількох простих зауваженнях, як вберегти себе від кіберзлочинів. А саме, до них належать: створення надійних паролів, захист інформації та періодична зміна паролів; поінформованість про розповсюджені прийоми, які використовують злочинці для того, щоб розпізнавати паролі; захист пристроїв та встановлення антивірусних програм; використання захищених мереж та перевірка своїх облікових записів.