УДК 004.056.5

Покотило О. А., асистент кафедри
Житомирський державний технологічний університет

АНАЛІЗ НОВИХ ЗАГРОЗ КІБЕРБЕЗПЕКИ ТА СПОСОБІВ ЗАХИСТУ ВІД НИХ

Сучасний світ та суспільство з кожним днем стають все більш комп'ютеризованими та технологічно-залежними. Якщо раніше співробітники були прив'язані до офісу, то тепер вони мають можливість працювати де завгодно, просто підключившись до серверу компанії із свого особистого пристрою. Це забезпечує не тільки більший рівень гнучкості, але і більшу ефективність працівників.

Такий підхід пропонує все більша кількість підприємств, що дає працівникам можливість виконувати роботу в більш комфортних умовах. Близько 35% підприємств у Європі в даний момент пропонують можливість своїм співробітникам працювати з дому.

Збільшення кількості цих людей ставить перед IT-відділами компаній складні питання забезпечення безпеки. Загальні витрати на цю сферу зростають із року в рік, а пробіли в системі безпеки IT обходяться все дорожче.

Насправді, існуючі ризики досить різноманітні, і втрата даних може виникати в різних формах, наприклад крадіжка пароля або навіть самого пристрою. Найбільший відсоток інцидентів безпеки в світі пов'язаний з «викраденням особистості». Такий кіберзлочин трапляється кожні дві секунди, і, в більшості випадків, основною його причиною є слабкі паролі.

Все це призводить до того, що злочинці можуть легко отримати конфіденційну особисту або корпоративну інформацію. Тому багато підприємств не використовують в повній мірі можливості позаофісної роботи співробітників, адже інноваційні рішення, які мали б захищати працівників, можуть призвести до нових ризиків та загроз.

Загрози інформаційної безпеки набувають нового вигляду. Це стосується трьох типів задач, які мають вирішувати засоби захисту, включаючи загрози конфіденційності, цілісності та доступності:

– порушення роботи системи та інфраструктури, що забезпечує її підтримку;

– крадіжка інформації;

– загрози, які можуть виникнути внаслідок використання ненадійного захисту конфіденційної інформації.

Із загрозами інформаційної безпеки стикається практично кожен. Значні ризики представляє собою шкідливе ПЗ (віруси, черви, троян-

ські програми, програми-вимагачі), фішинг (отримання доступу до логінів та паролів користувача) і крадіжка особистості (використання чужих персональних даних). Метою кібератаки можуть стати навіть акаунти в соціальних мережах чи додатках, дані банківських карт чи паспортні дані. Крім того, зловмисники активно займаються освоєнням нових сфер, таких як робототехніка, штучний інтелект та інтернет речей (IoT).

Для того, щоб захиститись від нових загроз, необхідні і нові засоби захисту. Які б сподівання ми не покладали на антивіруси, встановлені на ПК, все одно вони залишаються вразливими до різних атак.

Сьогодні важко виділити якусь окрему передову технологію захисту інформаційної системи. Одними з найбільш надійних елементів системи захисту є багатокомпонентні і багатофакторні системи автентифікації, які можуть працювати як окремо, так і поєднуючись між собою. Серед них є стандартні, такі як сканери відбитків пальців, а є і більш нові, наприклад, захист на основі IP-адрес і GPS-трекеру.

Важливим в будь-якій інформаційній системі є забезпечення конфіденційності, цілісності та доступності інформації. Якщо і далі використовувати традиційну парольну автентифікацію для доступу до інформаційних ресурсів, то ризик виникнення кібератак збільшується, адже близько 80 відсотків інцидентів в сфері інформаційної безпеки виникає внаслідок використання слабких паролів.

Альтернативою є багатофакторна автентифікація, до переваг якої відноситься її можливість захисту інформації як від внутрішніх загроз, так і від зовнішніх втручань. Вона ґрунтується на спільному використанні декількох факторів автентифікації, що значно підвищує рівень безпеки.

Отже, безпека ПК залежить, в першу чергу, від самого користувача. Адже саме він приймає рішення про встановлення того чи іншого ПЗ, перехід по посиланню або завантаження файла. Ніяка стратегія безпеки не є абсолютно ідеальною.

Засоби, заходи протидії та політики безпеки мають бути ненав’язливими і не повинні негативно впливати на продуктивність користувачів. Єдиного засобу захисту бути не може. Очевидно, він ще буде доповнюватися і розширюватися, адже забезпечення інформаційної безпеки – це не готове рішення, а процес. І засоби захисту мають іти в ногу з загрозами, що еволюціонують, та забезпечувати ефективну протидію їм.