Покращення захищеності інформаційних систем у сучасних умовах

Через постійне вдосконалення і поширення кіберзагроз ключовим елементом інформаційної безпеки стає навчання персоналу і керівництва компаній.

Сучасний світ невід'ємно пов'язаний з інформаційними технологіями (ІТ): можливість отримувати інформацію та швидкість цього процесу впливають на наше реальне життя. У зв'язку з цим захист інформаційних систем (ІС) та систем керування технологічними процесами від кіберзагроз став одним з ключових завдань для успішного функціонування бізнесу. Це особливо актуально для України, яка живе та працює в умовах війни.

Обережно, APT

Наведемо приклад: спеціалісти ДССЗЗІ у своїх звітах підсумовують інформацію щодо атак на державні та комерційні ІС. Згідно з їхнім аналізом, у 2022 році загальна кількість зареєстрованих кіберінцидентів порівняно з 2021 роком збільшилась майже втричі, а нових унікальних вірусних сигнатур у таких атаках було виявлено понад 87 тисяч — у 18 разів більше за попередній рік. Причому головними цілями залишились фінансовий сектор та об'єкти критичної інфраструктури.

Ці атаки стали складним випробуванням для України. Витоки більшості з них — advanced persistent threats (APT), тобто угрупування висококваліфікованих хакерів, створені для виконання деструктивних дій у кіберпросторі; здебільшого вони проникають в інформаційні системи з метою саботажу та/або викрадення інформації. Найчастіше джерелами APT є спецслужби та установи, що фінансуються з державних бюджетів та мають стратегічні цілі.

Сценарій роботи APT зазвичай відповідає наступному життєвому циклу.

- Вибір цілі: державні органи, об'єкти критичної інфраструктури тощо.
- Пасивна розвідка, отримання інформації про публічні сервіси компанії (web, mail, git, vpn тощо), системи захисту ІС та користувачів. Збір відбувається через відкриті джерела (OSINT), корпоративні сайти/сервіси, соціальні мережі та спеціалізовані сервіси.
- Активна розвідка: сканування сервісів на вразливості в програмному забезпеченні (ПЗ) або архітектурі ІС.
- Аналіз даних та вибір вектора атаки.
- Підбір або створення інструментів (вірусів, експлойтів тощо), розроблення сценарію використання та побудова інфраструктури для атаки.
- Експлуатація вразливостей: використання експлойтів до знайдених вразливостей, відправка фішингових листів тощо з метою проникнення всередину ІС.
- Горизонтальне просування в ураженій ІС з пошуком вразливих внутрішніх сервісів, закріплення та створення легального каналу, який не буде привертати увагу спеціалістів відділів ІТ або інформаційної безпеки (ІБ).
- Вертикальне просування з метою отримання найвищого рівня привілеїв у системі, пошук і скачування таємної/конфіденційної інформації.
- Використання отриманих можливостей. Після досягнення результату цикл повторюється для виконання іншої задачі на іншій цілі.

Спеціалісти ДССЗЗІ виявили показову тенденцію до надання переваги спробам повторних атак. Хакери повертаються до попередніх цілей, які вони контролюють, і використовують їх як плацдарм для продовження експансії в інші пов'язані ІС.

Одним з головних — і перших у черзі на використання — інструментів атаки є соціальна інженерія: фішингові листи та повідомлення з вірусами, зорієнтовані на непідготовленого та вразливого користувача, який за звичкою перейде за посиланням або відкриє заражений вірусом документ у себе на комп'ютері. Є і інші чинники, що дозволяють зловмисникам отримувати доступ всередину ІС. Серед

них варто відзначити відсутність координації або взаємодії між відділами IT та ІБ, що призводить до несвоєчасного оновлення ПЗ — а цим можуть скористатись зловмисники.

Praemonitus, praemunitus — «попереджений означає озброєний»

Зазвичай ІБ можна поділити на дві рівноцінні складові частини: організаційну та технічну, які не працюють одна без іншої.

До організаційної складової захисту можна віднести:
- стратегію реагування на інциденти: розроблення плану реагування, що передбачає швидке виявлення й ізоляцію вірусів та відновлення;
- політику безпеки: розроблення політик безпеки, визначення правил доступу до інформації під час її обробки, переміщення та зберігання тощо;
- аудит та моніторинг — організація регулярної перевірки безпеки, моніторингу ІС для виявлення аномалій;
- фізичну безпеку — це організація захисту фізичного доступу до IT-інфраструктури;
- налагоджену ефективну взаємодію між відділами IT та ІБ.

Технічна складова більш об'ємна і включає в себе сукупність апаратно-програмних та програмних технічних засобів, які захищають ІС в цілому та її окремі елементи від несанкціонованих дій користувачів та зовнішніх зловмисників. Це сукупність рішень, головним завданням яких є надання адміністраторам ІБ можливості контролювати легітимність процесу доступу та обробки, переміщення інформації уповноваженими на це користувачами, а в разі порушення — вживати адекватних заходів для припинення порушення та унеможливлення його повтору в майбутньому.

Важливим чинником, що дозволяє суттєво підвищити захищеність ІС і є елементом організаційної складової, має бути налагоджена взаємодія між відділами IT та ІБ. Це — критичний елемент для безпеки та ефективності роботи ІС, а ключові аспекти цієї взаємодії такі.
- Розуміння загроз і ризиків. Головним функціоналом спеціалістів відділу ІБ є виявлення та оцінка загроз для ІБ компанії. Відділи ІБ повинні активно співпрацювати з відділами IT.
- Впровадження технічних заходів безпеки. Відділ ІБ сприяє впровадженню технічних рішень для захисту від загроз, які повинні бути інтегровані в інфраструктуру IT.
- Розроблення та впровадження політик безпеки.
- Моніторинг та виявлення інцидентів. Відділ ІБ веде моніторинг заходів безпеки та реагує на можливі інциденти.
- Реагування на інциденти. У разі інциденту важлива швидка та скоординована відповідь. Відділи IT та ІБ мають працювати разом, щоб виявити причини, взяти на контроль ситуацію та запобігти подібним інцидентам у майбутньому.
- Security Awareness. Спільна робота відділів ІБ та IT щодо навчання персоналу кібергігієні є надважливою. Це включає в себе організацію тренінгів, усвідомлення загроз та впровадження найкращих практик ІБ.

Щодо Security Awareness зауважимо, що навчання та тренінги треба проводити не тільки для рядових користувачів, а й для технічних спеціалістів, що обслуговують інформаційну систему, та керівництва. Тренінги для технічних користувачів мають включати в себе такі розділи:
- відділ IT як ціль атаки зловмисників;
- навчання стосовно небезпеки фішингу та соціальної інженерії;
- надання огляду сучасних трендів кіберзагроз, які можуть стосуватися ІС і, відповідно, безпосередньо стосуються відділу IT;
- навчання спеціалістів IT створювати важкі та унікальні паролі, там де можливо — використовувати мультифакторну автентифікацію, дотримуватися найкращих практик управління паролями;
- пояснення важливості вчасного оновлення ПЗ та систем для запобігання використанню вразливостей зловмисниками;
- навчання безпечному користуванню мобільними пристроями та впровадження заходів для захисту конфіденційної інформації на них.

Security Awareness для керівників має важливе значення для забезпечення ефективної безпеки в організації. Керівництво має бути повідомленим про загрози та брати активну участь у впровадженні стратегій безпеки. Ось деякі аспекти, які рекомендовано включити в програму Security Awareness для керівників:
- розуміння керівником кіберзагроз;
- стратегії керівництва;
- культура безпеки;
- важливість лідерства;
- фінансові видатки на ІБ;
- управління ризиками;
- відповідальність за дані;
- захист важливих елементів ІС;
- стратегії взаємодії з IT-відділом та ІБ.

Сьогодні, коли кіберзагрози дедалі більше вдосконалюються та розповсюджуються, Security Awareness став критичним елементом для забезпечення ефективної кібербезпеки в організаціях. Зростання кількості атак, високий рівень маскування загроз та умови роботи, що постійно змінюються, — усе це створює необхідність для постійного вдосконалення знань та навичок персоналу.

Security Awareness дозволяє досягти розуміння комплексної природи кібербезпеки, важливості лідерства в створенні культури ІБ та глибокої уваги до стратегічних рішень на рівні керівництва. Це — важлива ланка у ланцюжку захисту ІС, яка визначає успіх або невдачу в захисті інформації та ІС.

Компанія ***SNT Ukraine*** має великий досвід впровадження методів ***Security Awareness*** в бізнесові, цифрові та технологічні процеси компаній та установ. Звертайтесь до нас, і ми допоможемо вам створити надійну тріаду кіберзахисту: люди, технології та процеси почнуть працювати на вашу безпеку як єдине ціле.

Олександр САЛИВОН,
консультант з кібербезпеки
SNT Ukraine
+380(44)238–63–88
info@snt.ua, www.snt.ua