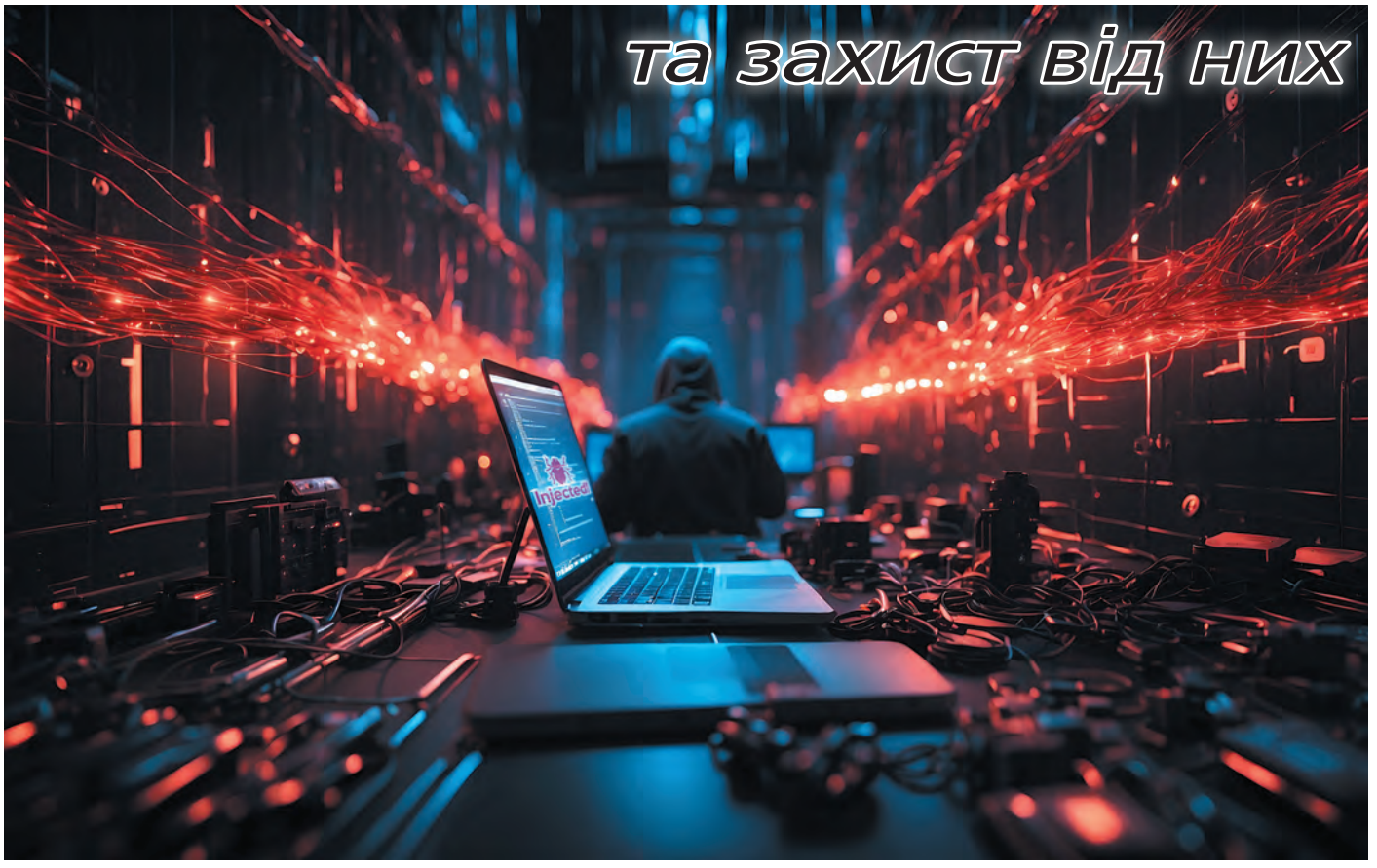
Атаки на ланцюжки постачання та захист від них



Supply chain attack — це підкоп під систему кібербезпеки організації. Зловмисне ПЗ проникає разом з легітимними інструментами.

Про явище під назвою Supply chain attack ми довідалися в 2017 році, коли NotPetya заблокував комп'ютери багатьох українських установ і організацій. За кілька років відбулась найпотужніша подібна атака в США — коли зламали платформу управління інфраструктурою Orion вендора SolarWinds. Злочинці інфікують виробників програмного забезпечення і через скомпрометовані продукти атакують їхніх клієнтів. Існує багато різновидів цих атак, але всі вони небезпечні, бо потенційними жертвами є всі замовники даного вендора.

«МтБ» розглянув найцікавіші атаки з залученням ланцюжків постачання, дізнався, що аналітики кажуть про тренди, і поцікавився прийомами захисту від цього типу атак.

Саєчка за переляк

У п'ятницю 19 липня компанія CrowdStrike випустила оновлення своєї програми Falcon Sensor, яка збирає телеметрію щодо можливих нових технік зловмисників. Файл оновлення, що містив помилку, спричиняв перехід комп'ютерів з Microsoft Windows до викидання «синього екрану смерті» (BSOD) і нескінченних перезавантажень. Найбільшого удару зазнали авіаперевезення: було скасовано тисячі авіарейсів, десятки тисяч — відкладено. За даними Microsoft, постраждало близько 8,5 млн комп'ютерів з Windows. В найскладніших випадках користувачі були змушені вручну видаляти бракований файл.

За повідомленням CrowdStrike, станом на 29 липня приблизно 99% сенсорів відновили роботу. Компанія оприлюднила детальні висновки розслідування, а також запевнила, що збій не створює вразливості. Проте експерти з кібербезпеки коментують, що ситуація підкреслює важливість управління ризиками в ланцюжку постачання. «Для більшості з нас автоматичні оновлення — це опція з малим ризиком. Але для великих підприємств, що мають критично важливі програми, — не таким вже малим. Внесення змін в критично важливі програми має бути більш виваженим, обережним і зворотнім», — написав Вільям Г'ю Маррей, консультант SANS Institute. «Логічно буде поставитися до цього як до дружнього інциденту кіберздирництва і переглянути шляхи забезпечення стійкості у разі компрометації», — зазначив Гел Шпанцер, інший консультант тієї ж організації.

Статистика атак

Що стосується реальних (зловмисних) атак через ланцюжки постачання, то їхня динаміка дуже коливається з року в рік. За даними компанії Statista, у 2023 році кількість користувачів, що постраждали від атак через ланцюжки постачання, глобально становила «усього лише» приблизно 138 тис. Це геть ніщо порівняно з понад 263 млн у 2019 році і навіть з 11 млн у 2022-му. Найбільш поширені прийоми злочинців — підробні листи, інфікування вебсайтів і встановлення зловмисного ПЗ.

Згідно зі звітом Identity Theft Resource Center, у 2022-му кількість витоків даних, спричинених атаками через ланцюжки постачання, значно (на 40%) перевищила кількість компрометацій через зловмисне ПЗ. Того року, зазначають дослідники, великі гравці у сфері кіберздирництва були здебільшого зайняті «конфліктом» в Україні, тож на перше місце вийшли атаки через ланцюжки постачання, які зачепили понад 10 млн людей і 1743 акаунти, які мали доступ до даних багатьох організацій. Для порівняння: від зловмисного ПЗ тоді постраждало 4,3 млн людей.

У грудні минулого року компанія BlueVoyant опублікувала звіт під назвою Supply Chain Defense Annual Global Insights Report. У ході дослідження було опитано понад 2 тис. посадовців з компаній, що представляли Північну Америку, Європу та Азійсько-Тихоокеанський регіон. Респонденти фіксували в середньому 4,16 проникнень через ланцюжки постачання з негативними наслідками для їхніх організацій (порівняно з 3,29 у 2022-му).

Погляд розробника

Атаки через ланцюжки постачання починаються з власне атак на самих постачальників з метою встановлення в їхні продукти зловмисного коду. Тут слабким місцем є те, що розробники ПЗ дедалі частіше використовують існуючі програмні компоненти, зокрема з відкритим вихідним кодом (OSS). За даними аналітичної компанії Enterprise Strategy Group by TechTarget (ESG), їхня доля в розробках вже становить 50%. Це дозволяє економити час і зусилля, проте створює нові безпекові ризики. Щоб оцінити проблеми, які через це виникають, і способи їх подолання, ESG опитала 368 фахівців з IT, кібербезпеки і програмування з різних організацій США і Канади, відповідальних за оцінювання, закупівлю і використання інструментів захисту для розробників ПЗ.

У своєму звіті «Зростання складності захисту ланцюжка постачання програмного забезпечення» (лютий 2024 р.) ESG повідомляє, що 91% опитаних нею компаній протягом минулого року зазнали інцидентів, пов'язаних з ланцюжками постачання ПЗ (**рис. 1**). З них 40% зіткнулися з тим, що хтось скористався вразливостями у сторонньому коді або хибно сконфігурованими хмарними сервісами. При цьому 96% зазнали того чи іншого негативного впливу через ці інциденти, найчастіше йшлося про встановлення програм для майнингу криптовалют і порушення угод про якість послуг, спричинене відновлювальними діями.

Найбільш вразливими елементами ланцюжка постачання ПЗ респонденти назвали програмне забезпечення з відкритим вихідним кодом (23%), репозиторії даних (21%), API (17%) і сторонній код або бібліотеки (8%).

При цьому дослідники відзначають, що у зв'язку з атаками через ланцюжки постачання велика більшість організацій (77%) «значно» посилила заходи захисту стороннього коду, і ще 22% зробили це в меншій мірі. З цих організацій 33% додали нові правила виявлення у системи контролю та/або аналізу безпеки, ще стільки ж запровадили сильну автентифікацію на кшталт мультифакторної для доступу до середовищ розробки і репозиторіїв вихідного коду. По 30% впровадили передінсталяційний аналіз ризиків для софту з відкритим кодом, посилили моніторинг працюючих застосунків і провели оцінювання існуючих засобів контролю на предмет того, чи здатні вони засікти подібну атаку.

Компанія ReversingLab у своєму звіті The State of Software Supply Chain Security 2024 робить висновок, що у 2023 році бар'єр для тих, хто хоче проводити атаки через ланцюжки постачання типу знизився і, ймовірно, знижуватиметься

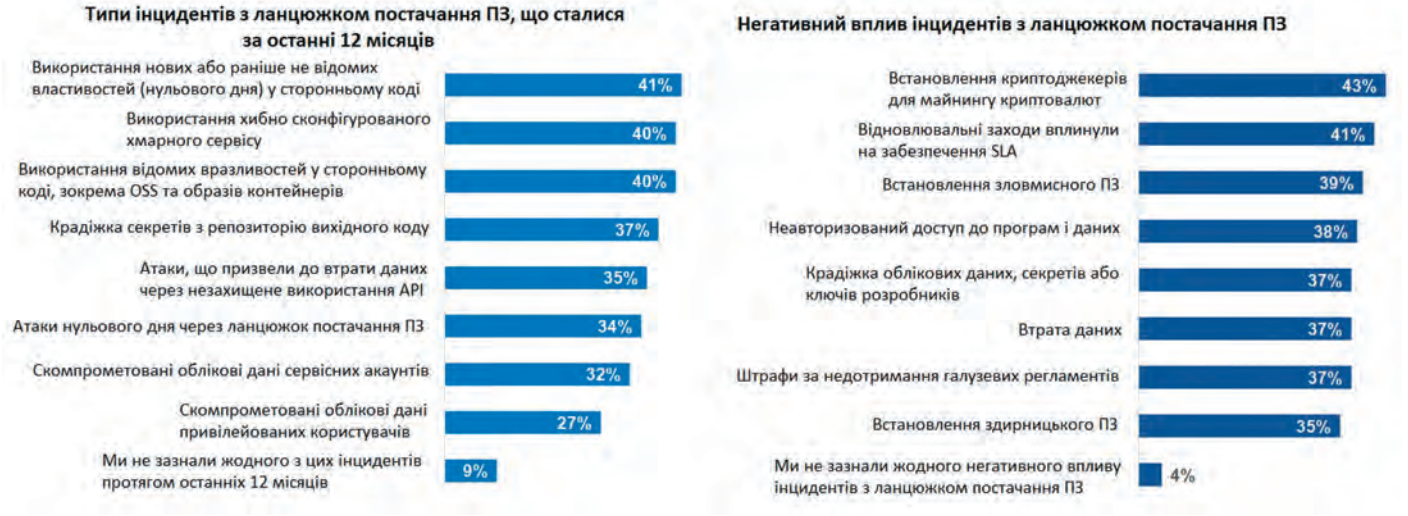


Рис. 1. Інциденти, пов'язані з ланцюжком постачання, та їх негативний вплив (джерело: TechTarget)

далі. Пов'язано це з дедалі більшим поширенням зловмисних пакетів на платформах OSS-коду. За перші 9 місяців 2023 року ReversingLab нарахувала на 28% таких пакетів більше порівняно з аналогічним періодом попереднього року. Кількість загроз, які циркулюють у репозиторіях відкритого коду, у період з 2020-го по 2023-й роки зросла на 1300%.

Також ReversingLab відзначає, що коло гравців, які займаються supply chain-атаками, продовжує розширюватися. З одного боку, це державні хакери, як-от північнокорейське угрупування Lazarus Group, яке здійснило кампанію під умовною назвою «VMConnect», використовуючи кілька десятків заражених пакетів Python. З іншого боку, якщо раніше supply chain-атаки можна було вважати золотим стандартом витончених кібернаступальних кампаній, що їх провадили найбільш умілі злочинці, то нині вони доступні навіть аматорам (script kiddies), які використовують платформи відкритого коду. У 2023 році supply chain-атаки нарешті «досягли дна кібернаступальної діжки»: з'явились готові, автоматизовані програмні продукти для атак, які продаються на чорному ринку.

Зловмисники, зазначає ReversingLab, намагаються скористатись прогалинами у можливостях моніторингу і виявлення загроз, через які розробники ПЗ та їхні клієнти не помічають ознак втручання в код і в процеси розроблення. Злочинці використовують механізми обфускації коду і малопоширені мови програмування, ховають зловмисний код у скомпільованих двійкових файлах.

SolarWinds

2020-й рік запам'ятався не лише коронавірусом, а й, можливо, наймасштабнішою кібератакою через ланцюжок постачання, яку взагалі можна було б вважати еталонною серед таких атак. Компанія SolarWinds спеціалізується на інструментах для моніторингу мереж та інфраструктури, зокрема вона має в своєму портфелі систему моніторингу продуктивності IT-систем під назвою Orion. Для своєї роботи вона потребує привілейованого доступу до систем в цілях збирання даних, через що й стала ласою ціллю для хакерів.

Злочинці проникли в мережу SolarWinds здогадно у вересні 2019 року. Наступного місяця вони ввели в Orion тестовий код, а у лютому 2020-го — робочу версію під назвою Sunburst. У березні SolarWinds почала розсилати оновлення Orion, що містило зловмисний код, який потенційно могли встановити понад 18 тис. користувачів (загалом на момент атаки SolarWinds обслуговувала понад 30 тис. державних та приватних організацій). Цей код міг передавати і запускати файли, здійснювати профілювання системи, робити перезапуск і відключати системні служби. Використовуючи цю лазівку, хакери отримали доступ до IT-систем клієнтів SolarWinds і можливість встановити вже туди своє шпигунське ПЗ.

Компанія FireEye, яка першою виявила Sunburst — аж у грудні 2020-го, — за результатами розслідування з'ясувала, що троян приховував свою діяльність, імітуючи трафік протоколу Orion, а також вмів ідентифікувати процеси, пов'язані з діяльністю антивірусів та рішень з розслідування інцидентів. Перш ніж зв'язатися з сервером командування і контролю, Sunburst здійснював низку перевірок. Завдяки цьому всьому троян зміг більше року залишатися непоміченим.

Втім, як пізніше з'ясувалося, наслідки атаки (принаймні видимі) були досить обмеженими. Хоча серед жертв були федеральні та місцеві держоргани США, компанії Microsoft, Intel, Cisco, Deloitte, сам FireEye та інші, у 2021 році SolarWinds повідомила, що насправді хакнутих користувачів було менше сотні. Решта або завантажили версію без трояна, або отримали інфіковану, але на сервери без доступу до Інтернету, або ж з якоїсь причини цей троян не встановив зв'язок з сервером командування і контролю. У всіх інших продуктах SolarWinds зловмисного коду не знайшлося. Microsoft повідомила, що хакери переглядали вихідний код кількох продуктів, але скачали тільки «деякі підгрупи» компонентів Azure, Exchange та Intune. Загалом чого хакери хотіли і яку інформацію ще поцупили, достеменно не відомо.

Адміністрація президента Байдена звинуватила в атаці російську Службу зовнішньої розвідки (СВР). Росіяни заперечили, заявивши, що «Росія не проводить наступальних операцій у кіберпросторі». Також у лютому 2021 році Reuters повідомляв про іншу, окрему атаку проти SolarWinds, цього разу з підозрою на китайських державних хакерів — серед жертв був «Національний фінансовий центр», федеральна агенція з розрахунку заробітних плат у складі департаменту сільського господарства, яка зберігала дані про тисячі держслужбовців.

Атака мала фінансові наслідки конкретно для SolarWinds. Forbes повідомляв, що компанія мусила сплатити $26 млн за одним з судовим позовом від інвесторів. У жовтні 2023 року, майже через три роки після скандалу, комісія США з цінних паперів та бірж висунула власний позов проти SolarWinds, заявивши, що компанія «ввела в оману інвесторів стосовно своїх практик кібербезпеки і відомих ризиків».

У будь-якому випадку найважливішим наслідком атаки можна назвати те, що вона підштовхнула до змін в індустрії кіберзахисту. Як зазначає TechTarget, багато комерційних і урядових організацій заходилися вигадувати нові методи реагування на такі атаки. Мати мережевий екран вже не достатньо: треба активно шукати вразливості в системах і або закривати їх, або перетворювати на пастки для хакерів.

Інші атаки

Sunburst, можливо, найбільш відома supply chain-атака, але й відтоді, і раніше було багато інших. Про NotPetya тут розповідати не будемо, бо та історія добре відома українцям. Тим більше що інших прикладів не бракує.

У 2017 році було атаковано ***CCleaner*** — популярний інструмент оптимізації та очищення операційних систем. Тоді інфікований застосунок завантажили або оновили більш ніж

2,3 млн користувачів. Заражена версія викрадала дані користувачів і відсилала їх на сервер командування і контролю.

Avast, який у липні 2017 року купив компанію Piriform — розробника цього застосунку — виявив, що хакери проникли в мережу Piriform щонайменше за п'ять місяців до того, як замінили оригінальну збірку версією з бекдором. Як з'ясувалося, хакери отримали доступ до комп'ютера одного з розробників за допомогою інструмента віддаленого контролю TeamViewer, ймовірно, використовуючи раніше вкрадені облікові дані цього користувача, і встановили зловмисне ПЗ. Після цього вони проникли в інший комп'ютер, підключений до тієї ж мережі, і відкрили бекдор з використанням протоколу Windows RDP. А далі по черзі встановили кілька зловмисних програм і розмістили на веб-сайті інфіковану версію CCleaner.

У вересні, більш ніж за місяць після початку поширення, дослідники Cisco Talos виявили цю інфіковану версію, і за три дні Avast за допомогою ФБР закрив сервер зловмисників. Проте ті встигли інсталювати ПЗ другої хвилі на 40 комп'ютерів великих міжнародних компаній.

У 2018 році атаки зазнав тайванський виробник мікросхем ***TSMC***. Атаку було здійснено варіантом здирницького ПЗ WannaCry, сплеск поширення якого припав на травень 2017 року. Вірус швидко поширився на 10 тис. машин компанії і зупинив виробництво чипів для нової лінійки «айфонів». Зараження відбулось внаслідок того, що «постачальник встановив у мережі TSMC інфіковану програму, не просканувавши на віруси».

У листопаді 2021 року стало відомо про оригінальну атаку на компанію ***Panasonic***. Як повідомляв сайт TechCrunch, внутрішнє розслідування за участю «стороннього консультанта з безпеки» показало, що «третя сторона» нелегально проникла на файловий сервер у Японії через сервер в іноземній філії. Сам злам стався ще у червні того року. Після виявлення несанкціонованого доступу Panasonic негайно запровадив додаткові заходи безпеки, зокрема посилив контроль доступу з-за кордону і моніторинг доступу. Проте під час інциденту проглядались персональні дані щодо деяких кандидатів на робочі місця і інтернів.

З більш свіжих прикладів можна назвати атаку на MOVEit — рішення для керованої передачі файлів, розроблене британською компанією Progress Software. У 2023 році російське здирницьке угрупування Clop скористалося вразливістю нульового дня у цій програмі. За даними компанії Emsisoft, яка досліджувала цей кейс, постраждали понад 2,7 тис. організацій і майже 96 тис. людей, здебільшого в США, хоча серед гучних імен були авіакомпанія British Airwaves і BBC.

У жовтні 2023 року зазнала хакерської атаки компанія Okta, виробник рішень для управління обліковими даними і доступом (IAM). Пікантності цьому випадку додає те, що зараження відбулось через одного зі працівників Okta, який увійшов у свій акаунт Google з робочого ноутбука і зберіг там свої облікові дані. Акаунт був вже був скомпрометований, імовірно, за допомогою фішингу або інших методів соціальної інженерії, розповідає у своєму блозі компанія ManageEngine (виробник SIEM Log360). Це дало змогу злочинцям отримати доступ до системи підтримки Okta і вилучити сесійні токени клієнтів, серед яких були компанії 1Password, BeyondTrust, Cloudflare та ще дві неназвані.

Наприкінці серпня 1Password сповістив Okta про підозрілу активність, але там вирішили, що 1Password став жертвою фішингу або зараження зловмисним ПЗ. Ще за кілька днів Beyond Security виявила і нейтралізувала атаку, спрямовану на акаунт адміністратора самої Okta, і передала ідентифікатор компрометації (IP-адресу). Okta знайшла відповідний службовий обліковий запис, заблокувала його і анулювала пов'язані з ним сесії.

Внутрішнє розслідування показало, що зловмисники отримали доступ до даних 134 клієнтів Okta, що загалом менше за 1%. Проте важливим був удар по репутації компанії як постачальника послуг з управління обліковими даними, і після цього витоку акції Okta впали на 11%. Більше того, постраждали і клієнти, які самі працюють у сфері кібербезпеки.

А ось зовсім свіжий приклад. Невдовзі після подій з CrowdStrike стало відомо про чергову атаку через ланцюжок постачання в США. Як повідомив ресурс Ars Technica з посиланням на кібербезпекову фірму Volexity, злочинці хакнули маршрутизатори неназваного інтернет-провайдера, після чого з їх допомогою підміняли відповіді DNS щодо легітимних адрес для завантаження оновлень щонайменше шести застосунків для Windows і MacOS. Оскільки сервери оновлень не використовують криптографічні сигнатури або шифрування для автентифікації з'єднань, злочинці мали змогу підміняти отриману адресу щойно вона потрапляла в інфраструктуру провайдера. В результаті на пристрій користувача завантажувалась версія застосунку з вбудованим зловмисним кодом (**рис. 2**).

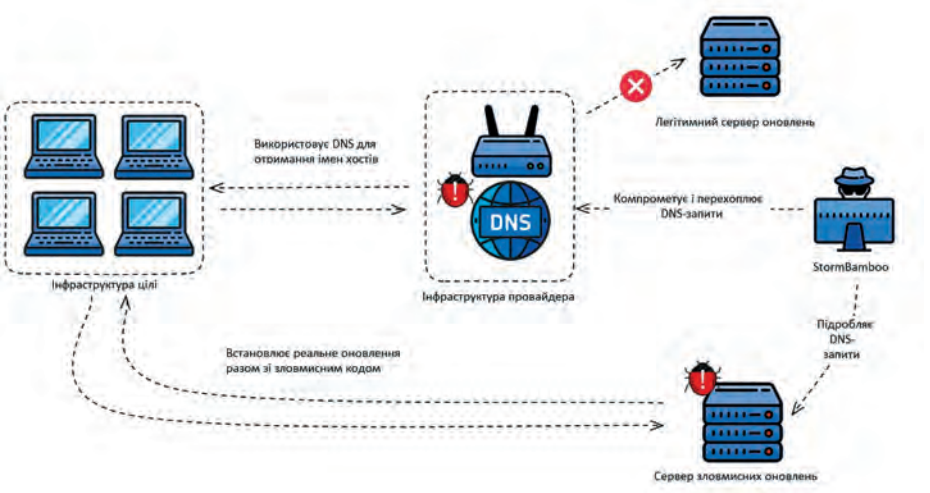


Рис. 2. Схема атаки з використанням фальшивого сервера оновлень (джерело: Volexity via ArsTechnica)

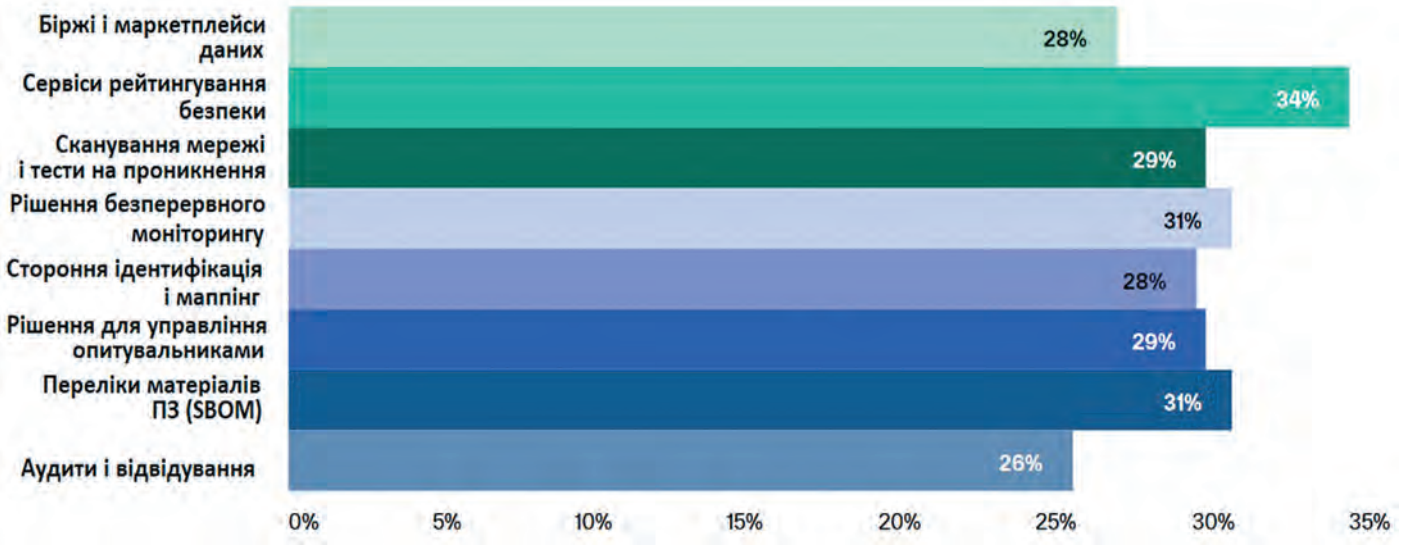


Рис. 3. Технічні рішення, що їх використовують компанії для управління ризиками, пов'язаними зі сторонніми продуктами (джерело: BlueVoyant)

Протидія

Як сказано у звіті BlueVoyant, компанії відчутно стурбовані supply chain-атаками і вживають заходів для запобігання їм. Власний досвід кіберзламів і новини про гучні атаки цього типу впливають на їхні практики кібербезпеки. 45% респондентів відповіли, що ці інциденти ймовірно призведуть до збільшення бюджетів на додаткові зовнішні ресурси для захисту проти кібератак через ланцюжки постачання. 51% очікують зростання бюджетів на відповідні внутрішні ресурси для захисту, і у 39% інциденти призвели до більш прискіпливого контролю з боку правління компаній.

Відсоток респондентів, які почали частіше перевіряти своїх постачальників на предмет кіберризиків (зокрема в реальному часі), сягнув 47% — на 42% більше, ніж у 2023-му. Також у 44% організацій щонайменше раз на місяць робляться доповіді для керівництва (порівняно з 38% у 2022-му).

В результаті компанії намагаються визначити оптимальне поєднання технологій, аналітики і аутсорсингових послуг для захисту ланцюжків постачання (рис. 3). З технічних рішень майже третина (31%) використовують перелік матеріалів програмного забезпечення (Software Bill of Materials — SBOM), який являє собою список усіх програмних компонентів з відкритим кодом і програмних компонентів третіх сторін, що присутні в базі коду. Цей, по суті, інвентарний опис не лише забезпечує облік компонентів, але й містить інформацію про їхні ліцензії та версії, а також про відомі вразливості.

Ще 31% використовують інструменти безперервного моніторингу, які дозволяють автоматично і в реальному часі відстежувати роботу застосунків, а також інфраструктури, мереж та програмних середовищ, на базі яких ці застосунки працюють. 29% компаній використовують інструменти управління опитувальниками, які автоматизують процеси анкетування постачальників для оцінювання ризиків. У частині послуг 34% організацій використовують сервіси рейтингування безпеки (security rating services — SRM). Вони здійснюють незалежне оцінювання стану кіберзахисту організації на основі структурованих даних про кіберзагрози (threat intelligence feeds), які знаходяться у відкритому доступі. Рейтинг складається у порівнянні з іншими організаціями і дозволяє побіжно оцінити стан власної кібербезпеки.

Конкретні поради від BlueVoyant такі. По-перше, організаціям варто допомагати вендорам: не просто сповіщати їх про вразливості і сподіватися, що вони щось зроблять, а співпрацювати для виправлення ситуації. По-друге, постійно відстежувати стороннє ПЗ, у разі проблем виявлення вразливостей сповіщати вендорів протягом кількох годин, а не днів, і тримати керівництво в курсі щодо управління ризиками. По-третє, ввести градацію вендорів за ступенем кіберризику і здійснювати їх моніторинг відповідно до цього ступеня. І, що не менш важливо, навіть ті співробітники, які безпосередньо не залучені до кіберзахисту, повинні розуміти, що сторонні програмні продукти впливають на стан кібербезпеки підприємства і становлять ризики, які можуть обернутися фінансовими і репутаційними втратами.

А ось прості поради від ManageEngine. Запровадити багатофакторну автентифікацію, яка додатково убезпечить облікові записи, навіть ті, що рідко використовуються, і заблокує злочинцям доступ до чутливої інформації. Навчати персонал розпізнавати фішингові атаки. Запровадити політику використання паролів, регулярно їх змінювати і обмежувати доступ до інформації на основі найменших привілеїв. Мати систему аналізу поведінки користувачів і сутностей (UEBA) з машинним навчанням для виявлення підозрілих дій.

Як бачимо, нічого особливо екзотичного. Важливо не те, як до вас залізли, а те, як не пустити злочинців далі.

Василь ТКАЧЕНКО, **МтБ**