9.6 Кібербезпека: загрози, рішення

У сучасному світі кібербезпека дуже важлива через різні загрози безпеці та кібератаки. Раніше потрібно було тільки встановити антивірус на комп'ютер, але сьогоднішні атаки є значно складнішими і вимагають спеціальних методів захисту. Для захисту даних безліч компаній розробили програмне забезпечення, яке захищає дані. Кібербезопаність важлива, тому що вона захищає не лише інформацію, а й усю робочу систему від вірусної атаки.

Кібербезпека – це практика захисту комп'ютерів, серверів, мобільних пристроїв, електронних систем, мереж та даних від шкідливих атак. Він також відомий як безпека інформаційних технологій чи електронна інформаційна безпека. Цей термін застосовується у різних контекстах, від бізнесу до мобільних обчислень, і може бути поділений на кілька загальних категорій. Рівень кіберзагроз постійно розвивається і стає все складнішим, і більшість компаній не мають власних інструментів кібербезпеки та можливостей підтримувати заходи безпеки в актуальному стані. Оскільки хакерам легше, ніж будь-коли, ініціювати атаку, організації тепер відчувають підвищений ризик та вищий рівень невизначеності. Згодом зломи та успішні атаки можуть коштувати компаніям мільйони, не кажучи вже про шкоду репутації бренду.

Безпека програм - використовується для тестування вразливостей програмних програм під час розробки та тестування, а також для захисту програм, що працюють у виробничому середовищі, від таких загроз, як мережеві атаки, використання вразливостей програмного забезпечення та атаки веб-додатків.

Мережева безпека - відстежує мережевий трафік, виявляє потенційно шкідливий трафік і дозволяє організаціям блокувати, фільтрувати або пом'якшувати загрози.

Хмарна безпека - реалізує заходи безпеки у загальнодоступних, приватних та гібридних хмарних середовищах, виявляючи та виправляючи неправдиві конфігурації безпеки та вразливості.

Безпека кінцевих точок - розгортається на кінцевих пристроях, таких як сервери та робочі станції співробітників, що дозволяє запобігати таким загрозам, як шкідливе ПЗ, несанкціонований доступ та використання вразливостей операційної системи та браузера.

Безпека Інтернету речей (IoT) – підключені пристрої часто використовуються для зберігання конфіденційних даних, але зазвичай не захищені конструктивно. Рішення безпеки IoT допомагають забезпечити прозорість та підвищити безпеку пристроїв IoT.браузера.

Аналітика загроз - об'єднує кілька каналів, що містять дані про сигнатури атак і суб'єктів загроз, забезпечуючи додатковий контекст для подій безпеки. Дані аналізу загроз можуть допомогти службам безпеки виявляти атаки, розуміти їх і розробляти найбільш відповідні заходи у відповідь.

Атака відмови в обслуговуванні. Відмова в обслуговуванні (DoS) атака перевантажує цільову систему з великим обсягом трафіку, що перешкоджає здатності системи нормально функціонувати. Атака за участю декількох пристроїв відома як атака розподіленої відмови в обслуговуванні (DDoS).

До методів DoS-атак належать:

HTTP-флуд DDoS - зловмисник використовує HTTP-запити, які здаються законними для перевантаження програми або веб-сервера. Цей метод не вимагає високої пропускної здатності або спотворених пакетів і зазвичай намагається змусити цільову систему виділяти якнайбільше ресурсів для кожного запиту.

SYN flood DDoS - ініціювання послідовності підключення по протоколу управління передачею (TCP) включає відправку SYN-запиту, на який хост повинен відповісти SYN-ACK, який підтверджує запит, а потім сторона, що запитує, повинна відповісти ACK. Зловмисники можуть використовувати цю послідовність, пов'язуючи ресурси сервера, відправляючи запити SYN, але не відповідаючи на SYN-ACK від хоста.

UDP flood DDoS - на віддалений хост закидається лавинне розсилання пакетів протоколу дейтаграм (UDP), що відправляються на випадкові порти. Цей

метод змушує хост шукати програми на порушених портах і відповідати пакетами Destination Unreachable, які використовують ресурси хоста.

ICMP Flood - потік пакетів ICMP Echo Request переповнює ціль, споживаючи як вхідну, і вихідну смугу пропускання. Сервери можуть намагатися відповісти на кожен запит пакетом відлуння ICMP, але не встигають за швидкістю запитів, тому система уповільнюється.

Посилення NTP - сервери Network Time Protocol (NTP) доступні всім і можуть бути використані зловмисником для надсилання великих обсягів UDP-трафіку на цільовий сервер. Це вважається атакою з посиленням через співвідношення запитів і відповідей від 1:20 до 1:200, що дозволяє зловмиснику використовувати відкриті сервери NTP для виконання великомасштабних DDoS-атак з високою пропускною здатністю.

Ін'єкційні атаки

Атаки з використанням ін'єкцій використовують різні вразливості для прямої вставки зловмисних даних у код веб-програми. Успішні атаки можуть розкрити конфіденційну інформацію, виконати DoS-атаку або поставити під загрозу всю систему.

Ось деякі з основних векторів ін'єкційних атак:

SQL-ін'єкція - зловмисник вводить SQL-запит у канал введення кінцевого користувача, такий як веб-форма або поле коментаря. Вразлива програма відправить дані зловмисника до бази даних та виконає будь-які команди SQL, введені в запит. Більшість веб-застосунків використовують бази даних на основі мови структурованих запитів (SQL), що робить їх уразливими для впровадження SQL. Новий варіант цієї атаки – атаки NoSQL, націлені на бази даних, що не використовують реляційну структуру даних.

Впровадження коду - зловмисник може впровадити код у програму, якщо вона вразлива. Веб-сервер виконує шкідливий код, якби він був частиною програми.

Впровадження команд ОС - зловмисник може користуватися вразливістю застосування команд для введення команд до виконання

операційною системою. Це дозволяє атаці захопити дані ОС чи захопити систему.

Впровадження LDAP – зловмисник вводить символи для зміни запитів LDAP. Система вразлива, якщо вона використовує необроблені запити LDAP. Ці атаки дуже серйозні, тому що сервери LDAP можуть зберігати облікові записи користувачів та облікові дані для всієї організації.

XML eXternal Entities (XXE) Injection - атака проводиться за допомогою спеціально сконструйованих XML-документів. Це відрізняється від інших векторів атак, оскільки використовує вразливості, властиві застарілим синтаксичним аналізаторам XML, а не неперевірені дані, що вводяться користувачем. XML-документи можуть використовуватися для обходу шляхів, віддаленого виконання коду та виконання підробки запитів на стороні сервера (SSRF).

Міжсайтовий скриптинг (XSS) - зловмисник вводить текстовий рядок, що містить шкідливий код JavaScript. Браузер цілі виконує код, дозволяючи зловмиснику перенаправити користувачів на шкідливий вебсайт або вкрасти файли cookie сеансу, щоб захопити сеанс користувача. Програма вразлива для XSS, якщо вона не дезінфікує дані, що вводяться користувачем, для видалення коду JavaScript.

Загрози кібербезпеки - це дії, що здійснюються особами зі шкідливими намірами, мета яких - викрасти дані, завдати шкоди або порушити роботу комп'ютерних систем. Загальні категорії кіберзагроз включають шкідливе програмне забезпечення, соціальну інженерію, атаки типу «людина посередині» (MitM), відмова в обслуговуванні (DoS) та атаки з використанням ін'єкцій.

Мета кібербезпеки - захистити дані, а також спрогнозувати, запобігти та пом'якшити наслідки будь-яких шкідливих впливів, які можуть завдати шкоди інформації (видалення, спотворення, копіювання, передача третім особам тощо).

До методів захисту відносять засоби, заходи та практики, які повинні захищати кіберпростір від загроз - випадкових чи зловмисних, зовнішніх та внутрішніх.

Кіберзагрози можуть виходити з різних джерел: від ворожих держав і терористичних груп до окремих хакерів і довірених осіб, таких як співробітники або підрядники, які зловживають своїми привілеями для скоєння зловмисних дій.

Загальні джерела кіберзагроз, яких відносять кілька поширених джерел для організаций:

- Національні держави - ворожі країни можуть запускати кібератаки на місцеві компанії та установи з метою завадити комунікації, викликати заворушення та завдати шкоди.

- Терористичні організації – терористи проводять кібератаки, спрямовані на руйнування чи зловживання критично важливою інфраструктурою, загрожують національній безпеці, підривають економіку та завдають тілесних ушкоджень громадянам.

- Злочинні групи. Організовані групи хакерів прагнуть зламати комп'ютерні системи з одержання економічної вигоди. Ці групи використовують фішинг, спам, шпигунське та шкідливе ПЗ для вимагання, крадіжки приватної інформації та онлайн-шахрайства.

- Хакери – окремі хакери націлені на організації, використовуючи різні методи атак. Зазвичай вони мотивовані особистою вигодою, помстою, фінансовою вигодою чи політичною діяльністю. Хакери часто розробляють нові загрози, щоб підвищити свої кримінальні здібності та покращити своє особисте становище у хакерському співтоваристві.

- Шкідливі інсайдери – співробітник, який має законний доступ до активів компанії та зловживає своїми привілеями для крадіжки інформації або пошкодження комп'ютерних систем з метою економічної чи особистої вигоди. Інсайдери можуть бути співробітниками, підрядниками, постачальниками чи партнерами цільової організації. Вони також можуть бути сторонніми, які зламали привілейований обліковий запис та видають себе за його власника.

Типи загроз кібербезпеці

Атаки шкідливого ПЗ

Шкідливе ПЗ - це ПЗ, яке включає віруси, черв'яки, трояни, шпигунське ПЗ та програми-вимагачі, і є найбільш поширеним типом кібератак. Шкідливе програмне забезпечення проникає в систему, як правило, через посилання на ненадійному веб-сайті або електронною поштою або через завантаження небажаного програмного забезпечення. Він розгортається в цільовій системі, збирає конфіденційні дані, маніпулює та блокує доступ до компонентів мережі, а також може знищити дані або повністю вимкнути систему.

Ось деякі з основних типів атак шкідливих програм:

- **Віруси** – фрагмент коду впроваджується у додаток. Коли програма запускається, запускається шкідливий код.

- **Черв'яки** - шкідливе ПЗ, яке використовує вразливість програмного забезпечення та бекдори для отримання доступу до операційної системи. Після встановлення в мережі черв'як може виконувати такі атаки, як розподілена відмова в обслуговуванні (DDoS).

- **Трояни** - шкідливий код або програмне забезпечення, яке видає себе за безневинну програму, що ховається у програмах, іграх або вкладеннях електронної пошти. Користувач, який нічого не підозрює, завантажує троян, дозволяючи йому отримати контроль над своїм пристроєм.

- **Програма-вимагач** - користувачеві або організації заборонено доступ до їх власних систем або даних за допомогою шифрування. Зловмисник зазвичай вимагає сплати викупу в обмін на ключ дешифрування для відновлення доступу, але немає гарантії, що сплата викупу фактично відновить доступ або функціональність. - Криптоджекінг - зловмисники розгортають програмне забезпечення на пристрої жертви і без їхнього відома починають використовувати свої обчислювальні ресурси для генерації криптовалюти. Зачеплені системи можуть стати повільними, а комплекти криптоджекінгу можуть вплинути на стабільність системи.

- **Шпигунське ПЗ** - зловмисник отримує доступ до даних користувача, що нічого не підозрює, включаючи конфіденційну інформацію, таку як паролі та

платіжні реквізити. Шпигунське програмне забезпечення може вплинути на настільні браузери, мобільні телефони та настільні програми.

- Рекламне ПЗ - активність користувача у браузері відстежується для визначення моделей поведінки та інтересів, що дозволяє рекламодавцям розсилати користувачеві цільову рекламу. Рекламне програмне забезпечення пов'язане зі шпигунським програмним забезпеченням, але не вимагає установки програмного забезпечення на пристрій користувача і не обов'язково використовується в зловмисних цілях, але може використовуватися без згоди користувача і ставити під загрозу його конфіденційність.

- Безфайлове шкідливе програмне забезпечення - в операційній системі не встановлено програмне забезпечення. Власні файли, такі як WMI та PowerShell, редагуються для увімкнення шкідливих функцій. Цю приховану форму атаки важко виявити (антивірус не може її ідентифікувати), оскільки компрометовані файли розпізнаються як легітимні.

- Руткіти - програмне забезпечення впроваджується у додатки, прошивки, ядра операційних систем або гіпервізори, забезпечуючи віддалений адміністративний доступ до комп'ютера. Зловмисник може запустити операційну систему у скомпрометованому середовищі, отримати повний контроль над комп'ютером та доставити додаткове шкідливе програмне забезпечення.

Головна увага приділена захисту інформації корпоративних та інших користувачів під час відвідування інтернет-сайтів, оплати рахунків та використання інтернет-банкінгу. Основними учасниками кіберпростору є користувачі (приватні та корпоративні) та оператори (мереж зв'язку та різних телекомунікаційних додатків). Під загрозу ставляться активи, які можна поділити на персональні та корпоративні, віртуальні та фізичні. Засоби реагування на кіберзагрози поділяють на превентивні, реактивні та які виявляють.

Також у сфері кібербезпеки використовується визначення «агент загрози» -людина або група людей, які виконують або підтримують атаку. Під

уразливістю активу розуміють слабку захищеність активу чи управління, яка може бути загрозою.

Окремо варто згадати термін «cybersafety», який не має прямого перекладу та розуміється як принципи безпечної поведінки у кіберпросторі. Дуже часто, користуючись інтернет-сервісами, соціальними мережами та іншими елементами кіберпростору, у людей виникає хибне уявлення про приватність і захищеність інформації, що міститься в кіберпросторі. Фото, відео, персональна інформація - все це розміщується в мережі для друзів, але може в будь-який момент використовуватися і зловмисниками. Саме тому безпечної поведінки в кіберпросторі потрібно починати вчити одночасно зі знайомством з комп'ютером.

Існує також таке поняття, як "інформаційна війна"; вона відрізняється від звичайної війни тим, що як зброя виступає старанно підготовлена інформація.

Важливо розуміти і той факт, що жодна система безпеки не здатна дати 100% гарантію захисту даних. І ця проблема, на жаль, актуалізується з кожним роком.

Під час пандемії було не до впровадження нових інструментів захисту, але найбільше мали інтерес до них. Конфіденційність перестала бути просто питанням відповідності вимог регулятора.

Основні пропоновані у стандарті методи оцінки та усунення ризиків:

1. Ідентифікація критичних активів: використання термінології кіберпростору розширюють область активів. Оскільки економічно нерентабельно захистити всі активи, важливо ідентифікувати критичні активи та передбачити спеціальні заходи для їхнього захисту. Виділення походить з контексту бізнесу, шляхом розгляду впливу втрати або погіршення активу на бізнесі в цілому.

2. Ідентифікація ризиків: учасники повинні розглянути додаткові ризики, загрози та атаки, що виникають при включенні в кіберпростір.

3. Відповідальність: учасник кіберпростору має нести додаткову відповідальність перед іншими учасниками.

4. Відключення систем та сервісів: якщо система або сервіс перестає використовуватись, то вони повинні бути видалені, що гарантує припинення впливу та зменшення загроз на пов'язані сервіси та інтерфейси.

5. Взаємодія: підхід до управління ризиками застосовується до всього кіберпростору. На учасників кіберпростору покладаються обов'язки планування на випадок непередбачених ситуацій, аварійного відновлення, розвитку та впровадження захисних програм для систем під їх контролем чи їх власності.

Головну загрозу надають штучні навмисні небезпеки. З огляду на дедалі більшу комп'ютеризацію всіх сфер бізнесу та зростання кількості електронних транзакцій ці загрози також бурхливо розвиваються. У пошуках способів отримання секретних відомостей та заподіяння шкоди компаніям, зловмисники активно використовують сучасні технології та програмні рішення. Їхні дії можуть завдавати значної шкоди, у тому числі у вигляді прямих фінансових втрат або втрати інтелектуальної власності.

Залежно від реалізацій, засоби захисту кібербезпеки бувають наступних типів:

Організаційні. Комплекс заходів та засобів організаційно-правового та організаційно-технічного характеру. До перших відносять законодавчі та нормативні акти, локальні нормативні документи організації. Другий тип – це заходи щодо обслуговування інформаційної інфраструктури об'єкта.

Апаратні (технічні). Спеціальне обладнання та пристрій, що запобігає витоку, що захищає від проникнення в IT-інфраструктуру.

Програмні. Спеціальне програмне забезпечення, призначене для захисту, контролю, зберігання інформації.

Програмно-апаратні. Спеціальне обладнання з встановленим програмним забезпеченням для захисту даних.

Найширше поширення сьогодні набули програмні засоби захисту інформації. Вони повністю відповідають вимогам ефективності та актуальності, регулярно оновлюються, ефективно реагуючи на актуальні загрози штучного характеру.

Для захисту даних у сучасних мережах застосовується широкий спектр спеціалізованого програмного забезпечення, серед яких можна виділити такі типи програмних засобів захисту:

Антивірусне ПЗ. Спеціалізований софт для виявлення, нейтралізації та видалення комп'ютерних вірусів. Виявлення може виконуватися під час перевірок за розкладом або запущених адміністратором. Програми виявляють та блокують підозрілу активність програм у «гарячому» режимі. Крім того, сучасні антивіруси можуть відновлювати файли, заражені шкідливими програмами.

Хмарні антивіруси (Cloud AV). Поєднання можливостей сучасних антивірусних програм із хмарними технологіями. До таких рішень відносяться сервіси Crowdstrike, Panda Cloud Antivirus, Immunet та багато інших. Весь основний функціонал ПЗ розміщений у хмарі, а на комп'ютері, що захищається, встановлюється клієнт-програма з мінімальними технічними вимогами. Клієнт вивантажує хмарний сервер основну частину аналізу даних. Завдяки цьому забезпечується ефективний антивірусний захист за мінімальних ресурсних вимог до обладнання. Рішення CloudAV оптимально підходять для захисту ПК, які не мають достатньої вільної обчислювальної потужності для стандартного антивірусу.

Рішення DLP (Data Leak Prevention). Спеціальні програмні рішення, що запобігають витоку даних. Це комплекс технологій, які ефективно захищають підприємства від втрати конфіденційної інформації з різних причин. Впровадження та підтримка DLP - вимагає досить великих вкладень та зусиль з боку підприємства. Однак цей захід здатний значно зменшити рівень інформаційних ризиків для IT-інфраструктури компанії.

Системи криптографії. (DES - Data Encryption Standard, AES - Advanced Encryption Standard). Перетворюють дані, після чого розшифровка може бути виконана тільки з використанням відповідних шифрів. Крім цього, криптографія може використовувати інші корисні програми для захисту інформації, у тому числі дайджести повідомлень, методи автентифікації, зашифровані мережеві комунікації, цифрові підписи. Сьогодні нові програми,

що використовують зашифровані комунікації, наприклад, Secure Shell (SSH), поступово витісняють застарілі рішення, що не забезпечують в сучасних умовах необхідний рівень безпеки, такі як Telnet та протокол передачі файлів FTP. Для шифрування бездротового зв'язку широко використовуються сучасні протоколи WPA/WPA2. Також використовується досить старий протокол WEP, який поступається з безпеки. ITU-T G.hn та інші провідні комунікації шифруються за допомогою AES, а автентифікацію та обмін ключами в них забезпечує X.1035. Для шифрування електронної пошти використовують такі програми як PGP та GnuPG.

Міжмережеві екрани (МСЕ). Рішення, які забезпечують фільтрацію та блокування небажаного трафіку, контролюють доступ до мережі. Розрізняють такі види фаєрволів, як мережеві та хост-сервери. Мережеві фаєрволи розміщуються на шлюзових ПК LAN, WAN та в інтрамережах. Міжмережевий екран може бути виконаний у форматі програми, встановленої на звичайний комп'ютер або програмно-апаратне виконання. Програмно-апаратний фаєрвол - це спеціальний пристрій на базі операційної системи з встановленим МСЕ. Крім основних функцій, міжмережеві екрани пропонують низку додаткових рішень для внутрішньої мережі. Наприклад, виступають як сервер VPN або DHCP.

Віртуальні приватні мережі VPN (Virtual Private Network). Рішення, що використовує у межах загальнодоступної мережі приватну мережу передачі та прийому даних, що дає ефективний захист підключених до мережі додатків. За допомогою VPN забезпечується можливість віддаленого підключення до локальної мережі, створення спільної мережі головного офісу з філією. Безпосередньо для користувачів VPN дає можливість приховувати розташування та захист дій, що виконуються в мережі.

Проксі-сервер. Виконує функцію шлюзу між комп'ютером та зовнішнім сервером. Запит, який надсилається користувачем на сервер, спочатку надходить на proxy і від його імені надходить на сервер. Повернення відповіді проводиться також із проходженням проміжної ланки - proxy. Перевагою є те, що кеш проксі-

сервера доступний для всіх користувачів. Це підвищує зручність у роботі, оскільки найчастіше запитані ресурси перебувають у кеші.

Рішення SIEM - системи моніторингу та управління інформаційною безпекою. Спеціалізоване ПЗ, яке перебирає функцію управління безпекою даних. SIEM забезпечує збирання відомостей про події з усіх джерел, що підтримують безпеку, у тому числі від антивірусного ПЗ, IPS, фаєрволів, а також від операційних систем тощо. Також SIEM виконує аналіз зібраних даних та забезпечує їх централізоване зберігання в журналі подій. На підставі аналізу даних система виявляє можливі збої, атаки хакерів, інші відхилення і можливі інформаційні загрози.