Як захистити хмару:

загрози і протидія

ТЕМА НОМЕРА

Інструментів для захисту хмарних ресурсів стає дедалі більше, але гарантувати цілковиту безпеку все одно складно.

Початок десятиліття ознаменувався прискоренням цифрової трансформації, коли пандемія змусила компанії та працівників перейти до віддалених та гібридних режимів роботи, а це, своєю чергою, зумовило міграцію корпоративних даних і програм до хмар. Коли ж лихі часи для світу минули, в Україні, як і сто років тому, все лише починалося. Після 24.02 вітчизняні компанії гарячково заходилися переносити свої навантаження, частково або повністю, на хмарні майданчики: як публічні, так і приватні.

Проте нові технології — це й нові ризики, в даному разі пов'язані з неавторизованим доступом до ресурсів, витоком даних, і порушенням роботи застосунків. Загалом природа загроз не змінилася, але з'явилось більше слабких місць. Частково їх закривають провайдери, але дещо мусять брати на себе користувачі, насамперед шифрування даних і управління доступом

«МтБ» спробував дослідити, які небезпеки чигають у хмарах і за допомогою яких технологій з ними борються.

Чим далі в хмари, тим більше проблем

Влітку цього року компанія ***Palo Alto Networks*** оприлюднила звіт The State of Cloud-Native Security, підготовлений спільно з дослідницькою фірмою The Fossicker Group на базі опитування понад 2500 респондентів з 7 розвинених країн. Дослідження виявило, що організації продовжують мігрувати в хмари, насамперед задля створення нових і розширення існуючих продуктів та сервісів, а також для підвищення власної ефективності. Наразі 53% хмарних робочих навантажень цих організацій розміщені в публічних хмарах.

При цьому головними обставинами на шляху хмарної міграції є технічна складність, брак кваліфікованого персоналу, необхідність забезпечення усеосяжної безпеки, брак видимості сервісів та продуктів і необхідність дотримання регуляторних вимог. В середньому організації використовують понад 30 інструментів кібербезпеки загалом і 6–10 інструментів, які відповідають за захист хмар. При цьому 77% організацій важко визначити,

EcoStruxure™
Innovation At Every Level

Easy UPS 3-Phase Modular

Оптимальне по ціні ДБЖ з можливістю масштабованості

Нове високоефективне 3-фразне модульне ДБЖ для захисту критично важливих застосувань з можливістю заміни модулів в «гарячому» режимі (Live Swap).

- Потужність 50-250 кВт.
- Технологія самодіагностування.
- Інтегрована можливість віддаленого моніторингу та керування.
- Відмовостійкість.

www.se.com/ua

Life Is On | Schneider Electric

Рис. 1. Найпоширеніші інциденти безпеки у хмарах та на локальних ресурсах, 2023 рік (джерело: Statista)

які саме інструменти безпеки їм потрібні, і 76% відповіли, що наявні у них інструменти все одно залишають сліпі плями. Понад 60% опитаних організацій працюють у хмарах вже три або більше років, однак технічні складнощі і проблеми з забезпеченням усеосяжної безпеки досі стримують міграцію.

90% респондентів зазначили, що їхні організації не в змозі виявити, ізолювати і нейтралізувати загрозу впродовж першої години. Понад 30% назвали брак видимості головною перепоною для забезпечення усеосяжної безпеки, 25% мали справу з суттєвим порушенням регуляторних вимог. 39% повідомили про збільшення числа зламів, 30% — про суттєве збільшення числа спроб проникнення і часу незапланованого простою. У 42% організацій зросла середня тривалість усунення загроз, у 36% — час простою.

У звіті 2023 Cloud Security Report, який підготувала компанія Cybersecurity Insights на замовлення ***Check Point***, опитавши понад тисячу експертів з кібербезпеки, зазначено, що 76% організацій «вкрай» або «дуже» стурбовані хмарною безпекою. У той час як 39% респондентів повідомили, що понад 50% їхніх навантажень вже знаходяться в хмарі, більшість стикаються з браком фахівців з захисту хмар (52%) і захисту даних (58%) у мультихмарних середовищах. 24% респондентів мали принаймні один безпековий інцидент, пов'язаний з публічними хмарами, найчастіше з причини неправильного конфігурування, компрометації облікового запису або експлуатації вразливості.

Опитування показало, що 62% організацій використовують «хмарнонароджені» (cloud-native) інструменти для управління конфігураціями, тоді як 29% послуговуються спеціальними рішеннями класу CSPM (системи управління станом хмарної безпеки). 72% користувачів мають три або більше окремі рішення для конфігурування хмарних політик, що спричиняє проблеми з управлінням та безпекою.

Що стосується конкретно найнебезпечніших видів атак проти хмар і у хмарах, то кожен експерт має свою думку. Але на перше місце ставлять «старий добрий» DoS/DDoS, адже з його допомогою можна заблокувати доступ до сервісів. Зокрема DoS-атака проти гіпервізора може «покласти» всю хмарну інфраструктуру. Компрометація облікового запису (за допомогою фішингу або експлуатації вразливості) пускає зловмисника до ресурсів, до яких має доступ цей запис. В подальшому це дозволяє їм викрадати дані або, наприклад, використовувати хмарні обчислювальні ресурси для майнингу криптовалют.

Неавторизований доступ може мати і зловмисний інсайдер, що особливо важко виявити. Зловмисники можуть захопити віртуальну машину і використовувати її для запуску кібератак всередині хмари. Атаки можуть здійснюватись і під час «живої міграції», тобто коли провайдер переносить віртуальні машини з одного сервера на інший, не перериваючи їхньої роботи.

За даними Statista на жовтень 2023 року, найпоширенішим видом кібератак що у хмарах, що на землі залишається фішинг. Конкретно для хмар на другому місці таргетовані атаки проти них, на третьому компрометація облікових записів (**рис. 1**).

Українські реалії: технології захисту ті ж, що й на землі

Ми провели власне невеличке і обмежене дослідження, опитавши десять компаній — операторів датацентрів, а також дистриб'юторів та інтеграторів, які постачають і розгортають рішення з інформаційної безпеки. Насамперед ми поцікавились, які продукти і сервіси пропонують ці компанії у розрізі захисту хмарних ресурсів (**рис. 2**). Якщо не враховувати послугу резервного копіювання та резервного відновлення даних, яку надають датацентри, пропонуються більш-менш ті самі рішення, які використовуються локально: системи захисту робочих стацій (антивіруси і складні рішення типу EDR/XDR), системи захисту електронної пошти, системи захисту від DDoS-атак, різноманітні мережеві екрани, системи автоматизації виявлення інцидентів та реагування на них (SIEM, SOAR). Специфічних рішень для захисту хмар майже не виявлено.

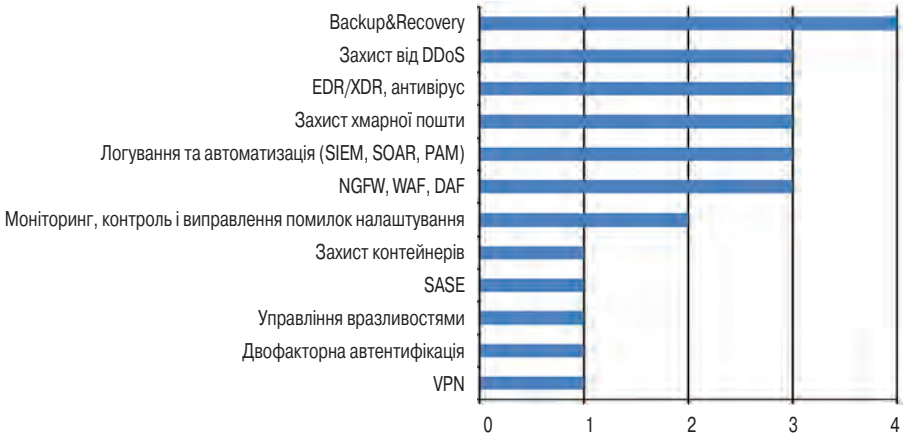


Рис. 2. Послуги та інструменти з захисту хмарних ресурсів, які пропонують українські компанії

ПОСИЛЮЙТЕ БЕЗПЕКУ РАЗОМ ЗІ SPAN

ЗВ'ЯЖІТЬСЯ З НАМИ:

Info.ua@span.eu

38 044 362 22 11

www.span.eu/ua

Компанія Span пропонує послуги з налаштування наступних рішень Microsoft:

УМОВНИЙ ДОСТУП MICROSOFT ENTRA ID (Azure Active Directory)

Зниження ризику компрометації облікових записів, контрольований доступ до застосунків

MICROSOFT DEFENDER FOR CLOUD APPS

Ефективний моніторинг використання хмарних сервісів, забезпечує повний захист SaaS, допомагаючи відстежувати та захищати дані

MICROSOFT DEFENDER FOR ENDPOINT

Контроль інфраструктури, протидія складним загрозам, оповіщення з єдиної уніфікованої платформи

MICROSOFT EXCHANGE ONLINE

Співіснування наземного і хмарного поштових сервісів та можливість оперативного переносу поштових скриньок

MICROSOFT PURVIEW INFORMATION PROTECTION

Класифікація та захист конфіденційної корпоративної інформації

MICROSOFT INTUNE

Безпечний доступ до корпоративних додатків/даних для співробітників, які використовують у роботі BYOD

MICROSOFT DEFENDER FOR IDENTITY

Виявлення скомпрометованих облікових записів та підозрілих дій всередині наземної інфраструктури Active Directory

MICROSOFT DEFENDER FOR OFFICE

Захист електронної пошти та Microsoft Teams від фішингу, небажаної пошти та небезпечного вмісту повідомлень

MICROSOFT PURVIEW INSIDER RISK MANAGEMENT

Виявлення підозрілих дій користувачів відносно корпоративних даних

АУДИТ ПОТОЧНОЇ ІНФРАСТРУКТУРИ

Експертні рекомендації щодо оптимізації витрат, оцінки ризиків та вдосконалення як інфраструктури в цілому, так і окремих її елементів

Для нових замовників Span до 31.12.2023 діє спеціальна цінова пропозиція на всі перелічені послуги.

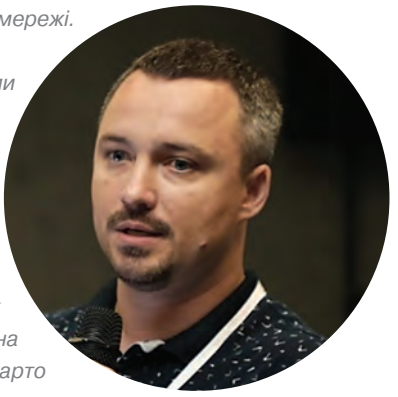
span

Microsoft Solutions Partner

Microsoft 2023 Partner of the Year

Хмарні середовища так само залежні від усіх існуючих інформаційних небезпек, як і наземні мережі. Специфіка хмари в тому, що замовники залежні від доступу до глобальної мережі, наявності стабільного з'єднання, безпечних каналів зв'язку, всі ці моменти дуже часто стають об'єктами атак зловмисників і перешкодою, а нерідко й репутаційними ризиками для компаній. Окремо слід звернути увагу на збільшення внутрішніх загроз через війну, пов'язані з інсайдерами та дедалі більшим впливом браку персоналу, що є вагомим аргументом за міграцію в хмари.

Оскільки, на нашу думку, найбільш вразливою ланкою при роботі з інформацією в хмарі є саме контроль доступу до інформації, в майбутньому на перше місце вийде використання штучного інтелекту для обходу систем контролю. Генерація голосу, зображень, поведінкових патернів значно ускладнить процес ідентифікації користувача. Також технології ШІ виведуть на новий рівень використання вже існуючих технологій, наприклад фішингу. Окремим пунктом варто виділити збільшення генерації за допомогою ШІ різноманітного шкідливого ПЗ, яке буде постійно ускладнюватись для унеможливлювання його виявлення.



Максим АНОШКО,
технічний директор компанії NWU

На запитання щодо запитів клієнтів відповіді дуже сильно розійшлись. Називались як технічні рішення (захист хмарної пошти, анти-DDoS, мережеві екрани, управління кінцевими пристроями тощо), так і організаційні, як-от: підвищення зрілості інформаційної безпеки, забезпечення безперешкодного доступу до ресурсів, простота та зручність керування системами безпеки тощо.

Як можна зрозуміти з відповідей датацентрів, ЦОД може насамперед запропонувати окремий рівень захисту у вигляді резервного копіювання та відновлення даних, в іншому ж захист хмарного середовища не надто відрізняється від захисту «на землі», з тією різницею, що частину функцій бере на себе постачальник послуг. Приміром, ***GigaCloud*** пропонує клієнтам послуги контролю за їхньою інфраструктурою через продукти VMware, які дозволяють бачити, як саме вона працює, та виявляти аномалії. На рівні провайдера діє система логування всіх подій та кроків адміністрування (PAM та SIEM), на основі якої відбувається виявлення та інформування про аномалії. Систему можна використовувати також на клієнтському рівні. Система управління вразливостями надає можливість оперативно реагувати на появу нових експлойтів. На рівні L5-L7 OSI компанія надає клієнтам можливість захищати свої сервіси, використовуючи продукти від VMware/Cisco/MikroTik, а на L3-L4 — послуги анти-DDoS, які називає наразі найпопулярнішими.

Датацентр «Парковий» використовує двофакторну автентифікацію на базі рішень Microsoft і Cisco з використанням мобільного додатка, інтегроване рішення Cisco для віддаленого доступу з шифруванням з'єднання між інфраструктурою або робочим місцем і хмарою, а також NGFW і IDS/IPS. З початком підготовки до зими зріс попит на розміщення серверного обладнання в захищеному середовищі датацентру, резервне копіювання і післяаварійне відновлення, а також на організацію віддалених робочих місць — Desktop-as-a-Service (DaaS). Тому «Парковий» нещодавно анонсував послугу DaaS, яка дає змогу розгорнути роботу навіть для невеликих клієнтів чи ФОПів, яким потрібно рішення тут і зараз, без інвестицій у розширення інфраструктури чи забезпечення її роботи під час блекауту.

De Novo вважає найбільш затребуваними сервіси резервного копіювання і післяаварійного відновлення, які забезпечують універсальний захист від непередбачуваних загроз цілісності та доступності даних та сервісів. Тож датацентр пропонує біля десятка сервісів, адаптованих для вирішення специфічних завдань замовника «тут и зараз». В арсеналі є широка функціональність мережевої безпеки гіпервізора мережі VMware, зокрема цікаве рішення — розподілений міжмережевий екран (distributed firewall, DFW). А також віртуальні пристрої Cisco з функціональністю NGFW та IDS/IPS.

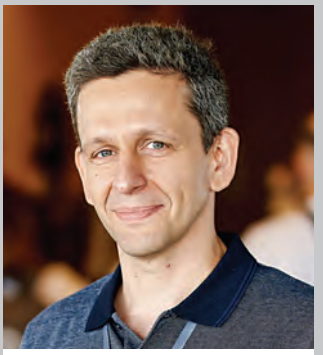
Київстар пропонує інструменти кібербезпеки на основі рішень Fortinet

ЧАСТИНУ ВІДПОВІДАЛЬНОСТІ БЕРЕ НА СЕБЕ ПРОВАЙДЕР

Найголовнішими універсальними загрозами є цілісність і конфіденційність даних. Зараз кількість кіберзагроз дійсно збільшилася, але це природно і пов'язано зі зростанням цифровізації бізнесу.

Хмарні ресурси простіше й зручніше захищати, адже частину цієї відповідальності переймає на себе провайдер. Власні ж ресурси доводиться моніторити й захищати самотужки, витрачаючи на це більше часу IT-команди. Провайдер має технічну компетенцію й чітко визначені правила безпеки для даних усіх клієнтів. Наявність у провайдера відповідних сертифікатів з безпеки є гарантією виконання ним своїх безпекових зобов'язань.

Майже всі компанії наразі розуміють, що їхня IT-стратегія повинна включати роботу з хмарами, і дедалі більше клієнтів уже навіть використовують декілька різних хмарних провайдерів, розподіляючи свою інфраструктуру між ними. Це правильне рішення, але воно має недолік: така інфраструктура є важчою для адміністрування і збільшує кількість точок ураження. Тому варто розглянути такі продукти, як Identity Access Management (IAM) для централізованого керування обліковими записами в різних системах різних провайдерів. А системи динамічної інвентаризації та системи управління вразливостями допоможуть контролювати периметр та розуміти, що саме потребує негайного захисту.



Володимир БЄЛОВ,
CEO GigaCloud Ukraine

і Microsoft. Зокрема: Email Security (захист корпоративної пошти від шкідливого ПЗ, фішингових атак, спаму та інших кіберзагроз), NGFW (захист від різнорівневих атак, фільтрація корпоративного трафіку), Web Application Firewall (захист веб-застосунків від шкідливого трафіку), EDR, резервне копіювання і аварійне відновлення важливої корпоративної інформації.

Ми поцікавились, які загрози хмарним ресурсам та інформації в компаніях вважають наразі найбільш небезпечними (**рис. 3**). Тут теж складно виділити якісь моменти, які турбують усіх, але більшість компаній вважають головною загрозою людський чинник. Три респонденти назвали загрозою помилки в налаштуваннях хмарних сервісах, два — зловмисні дії персоналу, один — ненавченість користувачів. З технічної точки зору хмарні сервіси залежать від стабільних і безпечних каналів доступу до них, а

ПОПИТ НА ВІДМОВОСТІЙКІСТЬ ЗНОВУ ЗРОСТАЄ

Якщо COVID спричинив попит на послуги, пов'язані з віддаленою роботою, то початок широкомасштабного російського вторгнення додав до цього ще міграцію IT-інфраструктур великої кількості організацій у хмару. Удари по енергетиці тільки підкріпили тренд розміщення у хмарі, де клієнту не страшні блекаути. Сьогодні цей тренд тільки посилився, доповнившись бажанням убезпечити функціонування бізнесу за рахунок географічного рознесення, тобто з розміщенням в локальному датацентрі і ЦОДі в ЄС.

З урахуванням цього на фоні підготовки до важкої зими відчутно зростає попит на рішення для забезпечення відмовостійкості роботи інфраструктури (розміщення серверного обладнання в захищеному середовищі ЦОД, IaaS саме в українських датацентрах) та побудови хмарної інфраструктури для організації віддаленої роботи (Desktop as a service). DaaS дозволяє швидко розгорнути віртуальні робочі місця для будь-якої кількості користувачів або, у випадку приватної особи або невеликої компанії, замовити робоче місце специфічної конфігурації – наприклад, з великою кількістю процесорів, швидкісним графічним адаптером і т. ін. Разом з цим знову стають досить популярними послуги резервного копіювання даних та побудови рішень з аварійного відновлення даних.

Серед трендів для кіберзлочинців ми бачимо використання хмар та AI для автоматизації та побудови майданчиків для зламу паролів, DDoS-атак і соціальної інженерії з метою отримання закритої інформації. Власники глобальних або приватних хмар будуть приділяти ще більше уваги аналізу кінцевих дій і сервісів, які експлуатуються користувачами. Тобто автоматизовані системи чи AI, інтегровані у хмарну екосистему, будуть вираховувати, чи не несуть дії користувачів всередині хмари шкоди іншим користувачам чи сервісам у цій або інших інфраструктурах.

Сергій КОЗЛОВ,
архітектор хмарних рішень
Датацентру «ПАРКОВИЙ»

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК ВИКЛИК ДЛЯ ХМАРНИХ ПРОВАЙДЕРІВ

Загрози будь-яким інформаційним ресурсам (не тільки хмарним) постійно зростають, і це пов'язано з а) збільшенням залежності нормального функціонування людської цивілізації від цих ресурсів; б) експоненційним зростанням складності інформаційних систем, що становить реальну загрозу можливості збереження розумного рівня контролю над ними. COVID чи війна можуть давати локальні сплески на основній лінії тренду, але це транзитивні фактори.

До загроз хмарним ресурсам треба віднести насамперед недосконалість архітектури хмари, зокрема використання технологічного стеку на базі відкритого ПЗ без комерційної підтримки рівня «підтримка продуктивних систем». Це міна, яка завжди рано чи пізно спрацьовує, і провайдер виявляється безпорадним: ресурсів власної команди недостатньо для вирішення проблеми, а звернутися нема до кого.

По-друге, нестабільність операційної моделі: надмірна кількість виключень зі стандартних процесів експлуатації хмари заради бажання задовольнити найрізноманітніші забаганки клієнтів, які, при детальному аналізі, найчастіше виявляються невиправданими, тобто завдання клієнта може бути вирішене цілком стандартним шляхом.

Третя проблема – «нормалізація девіації» хмарним провайдером, а саме – переоцінка ризиків у бік їх прийняття. Наприклад, відмова від впровадження технічних засобів захисту на кшталт IDS/IPS/SIEM та/або проходження сертифікації на відповідність стандартам інформаційної безпеки, зниження ступеню резервування обладнання чи вимог до кваліфікації персоналу. Все це з аргументацією «ну так вже за кілька років нічого ж не траплялось, а все перераховане ну дуже сильно впливає на собівартість, ми цього собі дозволити не можемо».

Геннадій КАРПОВ,
директор з технологій
дата-центру De Novo

Ключовою загрозою на найближче майбутнє є зсув компетенцій до сфери прикладних ландшафтів. Розробник «програмує в ноутбуці» і навіть не має уявлення про складність та особливості CI/CD pipelines, які доставляють зміни в коді до продуктиву. DevOps-інженер оперує сутностями на рівні «Kubernetes cluster», особливо не переймаючись деталями на рівні інфраструктури. Але значна (або навіть більша) частина загроз інформаційним системам та їхніх вразливостей знаходиться саме на інфраструктурному рівні. І відносна доля IT-професіоналів, які можуть дати цьому раду, зменшується.

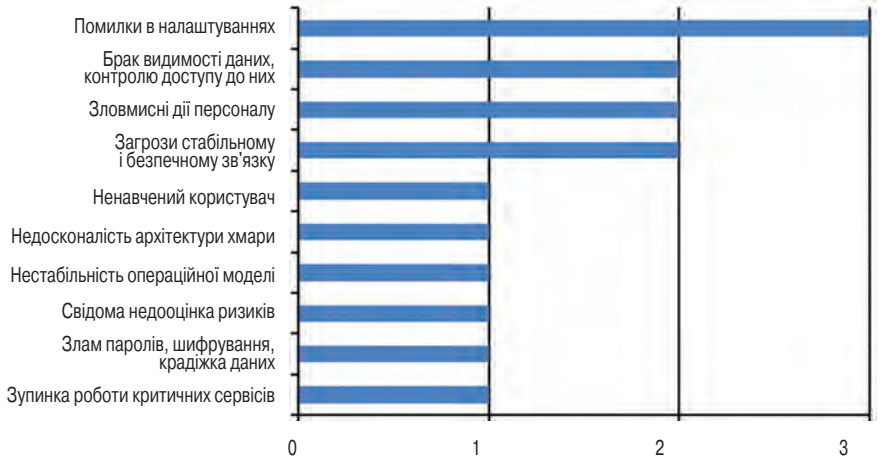


Рис. 3. Загрози хмарним ресурсам, що їх українські компанії вважають найбільш небезпечними

також від забезпечення видимості даних, які там зберігаються, контролю за ними, ізоляції цих даних і розмежування прав доступу до них.

Окремо ми задали питання про те, як змінились загрози хмарним ресурсам останніми роками у зв'язку спершу з пандемією, а потім повномасштабною війною (**рис. 4**). Тут насамперед компанії зауважують саме по собі збільшення кількості кібератак. Перехід компаній та працівників на віддалений режим роботи призвів до збільшення числа точок входу в периметр і підключених сторонніх застосунків, що також робить компанії більш вразливими. Зокрема респонденти звертають увагу на зростання числа DDoS-атак і атак проти державних установ та критичної інфраструктури.

У питанні про загрози, які можуть постати у найближчому майбутньому, респонденти також сильно розійшлися: по суті, кожен висловив власні занепокоєння. Насамперед це використання зловмисниками штучного інтелекту: для автоматизації атак, генерації шкідливого ПЗ, яке постійно змінюватиметься, обходячи механізми виявлення, а також для генерації голосу й зображень у цілях соціальної інженерії. Також фахівці зазначили атаки на пристрої IoT, які не мають належного захисту і часто стають слабкою ламкою в захисті

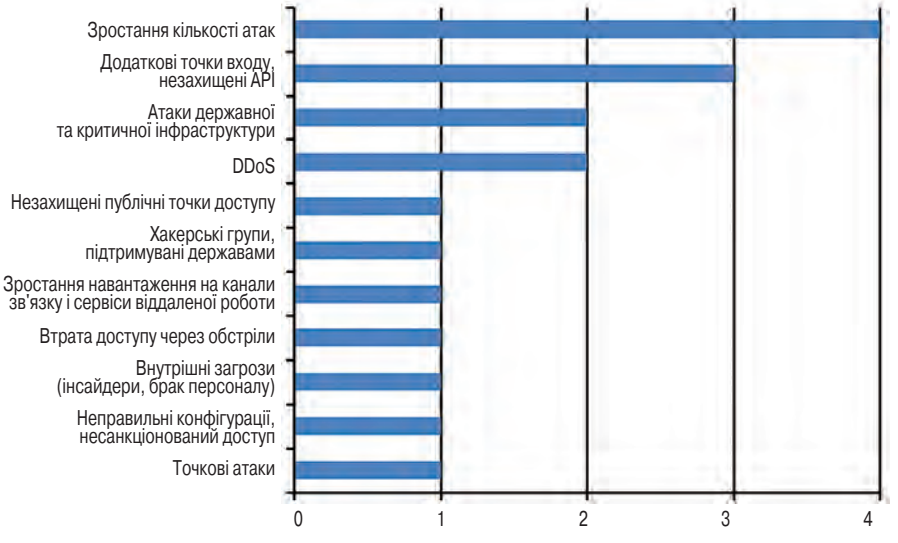
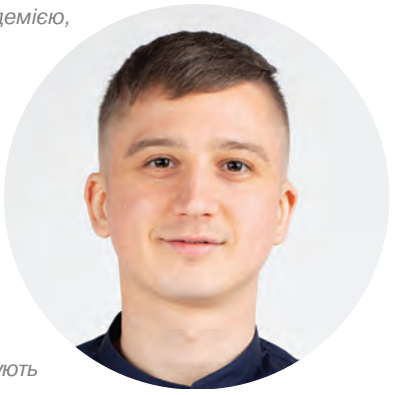


Рис. 4. Нові загрози хмарним ресурсам, пов'язані з пандемією та війною

Хмарна міграція, що була викликана пандемією, а потім повномасштабним вторгненням, стала причиною швидкого поширення загроз, які пов'язані з: 1) неправильними конфігураціями у хмарі, витоком даних та несанкціонованим доступом; 2) DDoS-атаками; 3) зламом акаунтів, незахищених програмних інтерфейсів (API).

На найближче майбутнє можна очікувати таких загроз:

1. Незаконний майнінг. Хакери використовують обчислювальну потужність хмар для майнінгу криптовалют, що буде досить дорого коштувати підприємству, оскільки рахунок сервіс-провайдер направить саме йому.



Володимир МІЩЕНКО,
менеджер з розвитку бізнесу по напряму кібербезпеки компанії WiseIT

2. Злам пристроїв «Інтернету речей». На жаль, більшість таких дистанційно контрольованих пристроїв не мають сучасного захисту, тому часто стають слабким місцем організації.

3. Повернення атак на базі соціальної інженерії. Нове покоління користувачів комп'ютерної техніки набагато більше знає і набагато менше вірить зловмисникам. Але генеративний штучний інтелект може перервати цей тренд вже завтра, підлаштовуючись під сучасну практику користування Інтернет-ресурсами.

організацій. Називались і інші загрози, які безпосередньо притаманні хмарі (атаки на контейнери і оркестратори, використання самих хмар для атак типу DDoS та зламу паролів, експлуатація інтеграції технологій віртуальної реальності і хмарних обчислень як точки входу в хмару, ускладнення розмежування доступу до даних різних користувачів).

Що стосується технологій захисту, які з'являться у найближчому майбутньому, то тут більшість опитаних назвала також штучний інтелект, який використовуватиметься для прогнозування та попередження загроз, аналізу великих масивів даних на предмет аномалій та підозрілої поведінки. На другому місці — модель Zero Trust для контролю не лише периметра, а й взаємодії між сервісами

Інструменти хмарного захисту

У царині захисту хмарних ресурсів вже створено різні класи cloud-native рішень, деякі з котрих є (принаймні в наших краях) екзотикою, а інші відомі деякий час, але все одно також ще досить екзотичні. Вони вирішують два головні завдання: по-перше, контролюють ресурси і програми, які знаходяться в хмарі (і то часто не в одній, а в кількох), на предмет вразливостей і неправильних конфігурацій, а по-друге — стежать, щоб користувачі не вчиняли зайвого. Далі буде багато абревіатур.

Перше з цих рішень — ***CASB*** (брокер безпеки доступу до хмар), своєрідний шлюз, який стоїть між інфраструктурою організації й публічними хмарами, посередник, який стежить за дотриманням політик безпеки. CASB забезпечує логування усіх дій з хмарними ресурсами (завантаження і вивантаження файлів, уведення облікових даних тощо), завдяки цьому організації бачать, де їхні дані і до кого вони могли потрапити. Окрім того, виявляє «тіньові IT-ресурси» — несанкціоновані програми — і класифікує їх відповідно до ризику, завдяки чому організації можуть їх дозволяти або забороняти. Також CASB може сам виявляти зловмисне ПЗ, використовуючи сигнатурний та поведінковий аналіз. CASB захищає дані при доступі до них з некерованих пристроїв (BYOD та інших), зокрема забезпечує шифрування даних, які зберігаються, і має функціональність DLP (карантин при доступі до файлів, «водяні знаки», які свідчать про власника, автоматичне видалення чутливих даних тощо).

В Інтернеті можна зустріти безліч рейтингів рішень CASB. Їх взагалі дуже багато, але з тих, які згадуються

У найближчий час найбільшою загрозою стане вартість хмарних послуг, яку потрібно буде сплачувати замовникам. Від початку активних бойових дій хмарні провайдери надавали свої сервіси безкоштовно. Замовники почали використовувати сервіси більш активно. Прийде час, коли за надані сервіси доведеться сплачувати комерційну ціну, і вона буде вражаючою для більшості компаній.

Необхідність зменшувати витрати може призвести до зворотної міграції інфраструктури у приватні датацентри. Ми знову отримаємо велику кількість гібридної інфраструктури, яку необхідно буде захищати, та відсутність бюджетів на такий захист.

Технології захисту розвиваються з погляду на поверхню атак інфраструктури та ризики, які може принести той чи інший тип атаки. Звісно, хмара надає нападникам швидкість у діях. Отже, сторона захисту повинна мати інструменти реагування у реальному часі. Тому найближчим часом ми побачимо зростання швидкості реагування на атаки, розвиток рішень для моделювання поверхні атаки та інструменти, що реалізують фреймворк Zero Trust у різних його проявах.

Роман ЧОРНЕНЬКИЙ,
керівник відділу продажу рішень з кібербезпеки ELKO Ukraine

найчастіше, можна назвати Microsoft Defender for Cloud Apps, Cisco Cloudlock, Netskope Cloud Security Platform, Palo Alto Next-Gen CASB, Skyhigh CASB, Broadcom Symantec Cloud SOC, Trend Micro Cloud App Security і Zscaler Internet Access.

Хмарний мережевий екран, який надається як послуга (і відповідно називається ***FWaaS***), може захищати і локальну інфраструктуру. Його переваги — здатність до швидкого масштабування, інтеграція з хмарною інфраструктурою, а також те, що за весь сервіс відповідає вендор. Послуги FWaaS пропонує багато виробників апаратних мережевих екранів, а також компанії, які працюють у сфері хмарної безпеки.

Інструмент управління правами доступу до хмарної інфраструктури (***CIEM***) — це засіб, який допомагає зрозуміти, які доступи існують в мультихмарному середовищі, і забезпечити в кожному випадку доступ з найменшими привілеями. CIEM автоматично перевіряє політики і конфігурації контролю доступу. Виявивши дозвіл, інструмент визначає, чи є відповідні привілеї доступу мінімально достатніми для виконання завдання, якщо ж привілей перевищує потреби, CIEM сповіщає оператора або вносить зміни автоматично. Для оцінювання CIEM використовує алгоритми машинного навчання і аналітику поведінки користувачів і сутностей (UEBA). Надання мінімально доступу з мінімально достатніми привілеями на час виконання завдання дозволяє скоротити поверхню атаки (**рис. 5**).

Вже згадані системи управління станом хмарної безпеки (***CSPM***) визначають ризики хмарній інфраструктурі (SaaS, PaaS, IaaS, безсерверні обчислення). Працюючи автоматично, CSPM регулярно сканує хмарні ресурси, ідентифікує

ОСНОВНІ ЗАГРОЗИ — ПОМИЛКИ НАЛАШТУВАННЯ І БРАК ВИДИМОСТІ

Перш за все, найбільшою загрозою хмарі є неправильно налаштовані параметри. Наприклад, нещодавній інцидент витоку 38 ТБ приватних даних у репозиторії Microsoft AI GitHub стався через один неправильно налаштований токен SAS.

Неправильно налаштовані доступи, відкриті ключі, надмірні дозволи облікових записів, неефективний захист ідентифікації, відкриті бази даних, кеш-пам'ять, неадекватна сегментація мережі та занедбана хмарна інфраструктура, – всі ці чинники створюють сприятливі умови для бічного переміщення по всій інфраструктурі. Таким чином зловмисник може використовувати інфраструктуру для власних потреб, спричинити витік даних або отримати доступ до мережі ваших партнерів чи клієнтів (supply chain).

За останніми дослідженнями світових аналітичних компаній, 82% порушень стосуються даних, що зберігаються в хмарі. Тож організаціям слід шукати рішення, які забезпечують комплексну видимість у гібридних середовищах і захищають дані під час їх переміщення між хмарними середовищами, базами даних, застосунками та сервісами.

Серед нових загроз, які постануть у найближчому майбутньому, першою, без сумніву, є штучний інтелект. Зловмисники вже використовують AI та ML для створення більш складних атак та для обходу захисту. До інших загроз треба віднести:

– віртуальну реальність. Для створення цих технологій активно використовуються хмарні обчислення. Через щільну інтеграцію VR може стати точкою входу в хмару;

– «Інтернет речей»;

– атаки на розширені Інтернет-протоколи. З розвитком нових протоколів, таких як IPv6 та HTTP/3, і переходом на них можуть з›явитися нові можливості для атак та зламу;

– атаки на хмарні контейнери та оркестратори (Docker, Kubernetes). Чим більше застосунків розгортається з використанням контейнерів, тим більшатиме кількість атак на них.

З іншого боку, хоча штучний інтелект можна використовувати для зловмисних цілей, він також буде потужним інструментом для захисників, допомагаючи їм підвищити свої навички, заощадити час і набрати швидкість.

Юрій ГАТУПОВ,
CEO ilT Distribution

Зросте популярність автоматизації. Використання автоматизованих засобів та оркестрації сприятиме кращому виявленню інцидентів, реагуванню на них та відновленню роботи.

Окрім того, набуватимуть популярності рішення для гігієни коду, а також рішення, які дозволять забезпечити захист програм чи нівелювати вразливості ще на рівні створення застосунків та коду. Це буде застосовуватися до всіх хмарних застосунків, контейнерів та оркестраторів.

ХМАРНІ РІШЕННЯ МАЮТЬ ВЛАСНИЙ ЗАХИСТ, АЛЕ МОЖЛИВІ ПРОБЛЕМИ З КОНТРОЛЕМ ДОСТУПУ

Не секрет, що виробники як хмарних enterprise-рішень, так і рішень з забезпечення їхньої безпеки від самого початку намагаються розробляти продукти з високим рівнем самозахисту від зламів. Якщо додати до цього так само високий рівень захищеності хмарних ресурсів (AWS, Azure, Google), на потужностях яких розгортається хмарна інфраструктура, стає очевидним зміщення фокусу загроз з технічного аспекту у напрямок невірних конфігурацій, людського фактору, в тому числі зловмисних дій персоналу з привілейованими правами. І такі ризики є найбільш серйозними.

Окрім зазначеного, є ще деякі загрози хмарним ресурсам та інформації. Проявились вони на початку ковідних змін, пов'язаних з масовим переходом до гібридного або повністю віддаленого режиму роботи. Це призвело до зростання навантаження як на канали провайдерів, так і на сервіси організацій для забезпечення віддаленої роботи, що знизило рівень та якість доступності хмарних ресурсів для кінцевих споживачів. З часом ситуація стабілізувалась, але російське вторгнення знову зробило питання втрати доступу до хмарної інформації актуальним через руйнування нашої енергетичної інфраструктури та можливе пошкодження вузлів і каналів передачі даних стратегічної важливості.

Загрози, які можуть екстремально зрости у найближчому майбутньому, пов'язані з ускладненням контролю розмежування даних різних замовників на стороні хмарних провайдерів (AWS, Azure, Google, IBM, Oracle). Складність хмарних технологій і сервісів, кількість їхніх користувачів, забезпечення дублювання / відмовостійкості між хмарними дата центрами, – усе це призводить до ускладнення процесу контролювання недоступності даних замовників для третіх осіб, а збільшення кількості витоків інформації саме через такий крос-доступ про це і говорить.

Сергій ГАННОЧКА,
директор з інформаційної безпеки компанії Intrasystems

З часом більшого поширення набуде процес переходу до мікросервісної архітектури на рівні провайдерів хмарної інфраструктури, а саме виробників хмарних же продуктів інформаційного захисту (так само, як це відбувається для веб-сервісів та веб-застосунків).

їх і визначає їхній статус, відшуковує неправильні конфігурації, вразливості і можливі порушення регуляторних вимог (наприклад, забагато користувачів мають доступ до бази даних). Про знайдені проблеми CSPM сповіщає оператора, а деякі рішення можуть самостійно вживати коригувальних заходів. Споріднені системи управління станом безпеки ***SaaS*** (***SSPM***), як видно з назви, зосереджені на убезпеченні користування робочими інструментами SaaS, такими як Office 365 або Google Docs. SSPM знаходить помилки налаштування безпеки, зайві доступи, непотрібні або неактивні облікові записи, ризики порушення регуляторних вимог та інші проблеми.

Платформи захисту хмарних навантажень (***CWPP***) пристосовані для захисту мультихмарних та гібридних інфраструктур, які поєднують публічні і приватні хмари й наземну мережу. За допомогою CWPP організації можуть аналізувати ризики, пов'язані з усіма навантаженнями, які там розміщені. CWPP радять впроваджувати разом з CSPM, при цьому остання контролюватиме саме хмарне середовище і облікові записи користувачів, а перша — програми, які в тому середовищі працюють.

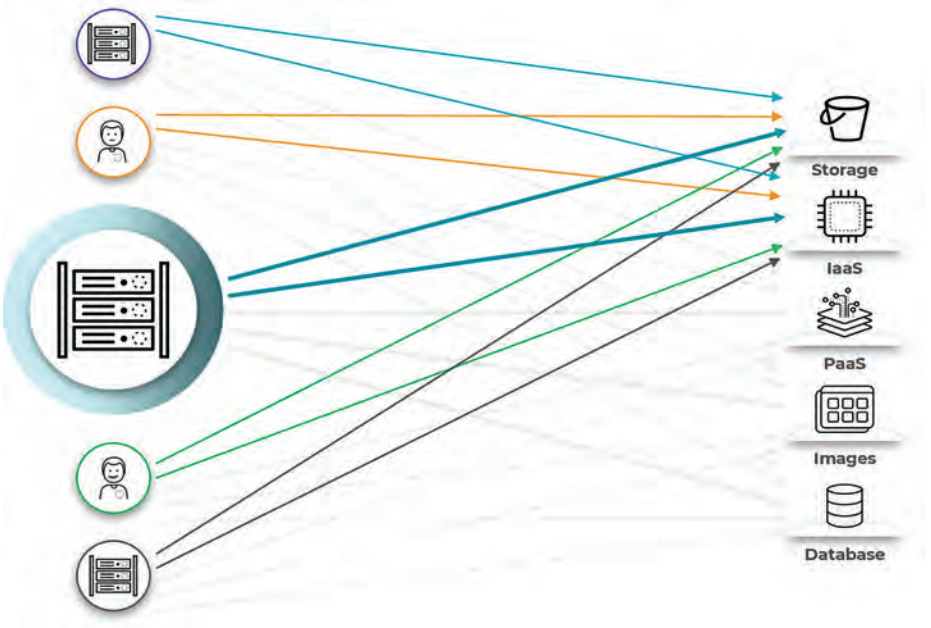


Рис. 5. Доступ з мінімально достатніми привілеями (джерело: Palo Alto Networks)

Інструменти статичного тестування програм (***SAST***) призначені для перевірки вихідного коду на предмет вразливостей на етапі його створення. SAST шукає у файлах секретні дані, такі як паролі і токени безпеки, відстежує вразливості у бібліотеках, веде реєстр сторонніх інструментів, які використовуються в процесі розроблення, аналізує поведінку цих інструментів (куди вони надсилають дані) і визначає можливі ризики. Аналізуючи програми без необхідності їх запуску, SAST вказує розробникам на помилки та інші проблеми, що дозволяє заощадити час і ресурси. Сучасні засоби SAST використовують алгоритми машинного навчання для виявлення вразливостей і секретних даних з меншою кількістю хибнопозитивних сповіщень. Загалом інтеграція кіберзахисту безпосередньо в процес розроблення коду дозволяє радикально зменшити подальші ризики.

Нам з хмарами жити, а тому всі ці інструменти захисту поступово ставатимуть нормою. З іншого боку, технології постійно розвиваються, і вже незабаром можуть з'явитись якісь нові ідеї та концепції. Зокрема пов'язані з інтеграцією в ці інструменти штучного інтелекту і машинного навчання.

Василь ТКАЧЕНКО, МтБ