Атака зсередини,
або про захист від інсайдерських загроз

Реалії такі, що організаціям треба стерегтися не лише хакерів, але й власних співробітників.

Інсайдерські загрози складно виявляти, а збитки від них можуть бути доволі великими. Ворожі агенти, власні незадоволені або просто недбалі працівники, ба навіть партнери, які мають доступ до мережі, — усі вони можуть спричинити витік чутливої інформації. Кількість інцидентів, пов'язаних з інсайдерами, постійно зростає, так само як і їх ціна.

Захист від інсайдерських загроз — це комплексні заходи, які включають в себе впорядкування інформації, встановлення шаблонів поведінки користувачів, управління правами доступу, навчання персоналу тощо. Існують спеціалізовані рішення, які беруть на себе технічний бік цієї справи. Розбираємося, як і за допомогою чого організації можуть уберегтися від шкоди, спричиненою зловмисними чи ненавмисними діями власних працівників.

Роззяви, незадоволені й шпигуни

Існує кілька видів джерел інсайдерських загроз, які різняться своєю мотивацією (ба навіть її відсутністю). Американська агенція з кібербезпеки та захисту інфраструктури (CISA) визначає інсайдера як особу, яка має авторизований доступ до ресурсів організації або знання про них, у тому числі про персонал, будівлі, обладнання, мережі та системи. Приклади інсайдерів — це власне співробітники компанії; інші особи, яким надано постійний доступ (представники підрядника, постачальника, ремонтної організації тощо); особи, які беруть участь у розробці продуктів та сервісів компанії; особи, які з тих чи інших причин володіють інформацією про функціонування компанії, її сильні та слабкі сторони, бізнесову стратегію та цілі, майбутні плани.

Інсайдерські загрози можуть бути цілком безневинними, спричиненими недбальством працівників, які ігнорують правила безпеки, або випадковістю (наприклад, відправили чутливу інформацію не на ту електронну адресу). Зловмисні інсайдери вчиняють дії задля особистої вигоди або через якусь образу на організацію. Окремим випадком є змова, коли зловмисний інсайдер діє в інтересах стороннього злочинця. Нарешті, небезпека може бути пов'язана зі сторонніми організаціями (партнерами або постачальниками), які можуть якимись своїми діями скомпрометувати безпеку компанії, або навпаки — через вже наявні вразливості можуть навмисно або ненавмисно спричинити негативні наслідки.

Gartner зазначає, що зумисні інсайдерські атаки часто рухаються за передбачуваною схемою. Співробітник припускається помилки і виправляє її; не відчувши жодних наслідків, він перевіряє, чи можна за бажання повторити цю помилку. Критичний момент настає, коли поєднання стресу і вад характеру спонукає працівника переосмислити ці взагалі-то шкідливі дії як корисні, необхідні задля вищої мети і т.д.

Згідно з дослідженням ***Ponemon Institute***, результати якого опубліковані у звіті 2022 Cost of Insider Threats Global Report, з-поміж зафіксованих торік 3807 інцидентів 56% були спричинені недбальством персоналу або контрагентів, що стало наслідком низки чинників: неубезпечення пристроїв, нехтування політикою безпеки та оновленням ПО. За даними дослідження, термін виявлення та ізоляції інциденту нині становить 85 днів — на 8 більше, ніж два роки тому (**рис. 1**). Лише 12% інцидентів було ізольовано менш ніж за 30 днів, тоді як у 34% випадків для цього знадобилось понад 90 днів. Зросла й частота інцидентів: 67% компаній повідомили, що впродовж року зазнали від 21 до понад 40 інсайдерських атак; у 2020 році таких було 60%, у 2018-му — 53%. Найбільша кількість зафіксованих інсайдерських атак в одній організації — 46.

Рис. 1 Середня тривалість виявлення та ізоляції інциденту, пов'язаного з інсайдерами (джерело: Ponemon Institute, 2022 р.)

З усіх інцидентів 26% були викликані зловмисними інсайдерами, і кожен з таких у середньому завдавав збитків на $648 тис. Найбільш руйнівними були інциденти, пов'язані з крадіжкою даних облікових записів (за допомогою фішингу та інших прийомів соціальної інженерії) — таких було 18%, і «коштували» вони в середньому $805 тис.

При цьому найбільші збитки обумовлені простоюванням бізнесу через зменшення продуктивності праці персоналу (про це повідомили 23% респондентів). Ще 21% випадків пов'язані з технологіями, у тому числі амортизованою вартістю і оплатою ліцензій за програмне і апаратне забезпечення, придбаного у відповідь на ці інциденти.

Також прикметно, що серед коштів, витрачених на подолання інсайдерських атак, найбільше витрачається на ізоляцію інциденту (в середньому $184,55 тис.) та подальшим розслідуванням ($128,056 тис.) і подоланням наслідків (майже $120 тис.). Водночас на заходи з моніторингу й спостереження витрачається усього $35 тис.

Компанія ***DTEX Systems*** у своєму звіті 2022 Insider Risk Report полезімує з Ponemon щодо статистики виявлення інсайдерських загроз. Якщо Ponemon повідомляє про зростання на 44% виявлених інцидентів кібербезпеки, спричинених інсайдерами, то DTEX стверджує, що реальна кількість таких інцидентів зросла на 72%. Ponemon оцінює середні річні збитки через відомі інциденти, пов'язані з інсайдерами, у $15,38 млн, DTEX же вважає, що реальні втрати набагато вище, ніж офіційно повідомляється. Ponemon у своєму дослідженні нараховував, що 23% виявлених інсайдерських атак були пов'язані з виведенням чутливих даних або інтелектуальної власності, але DTEX пише, що такі крадіжки мали місце у 42% інцидентів. Загалом випадки промислового шпигунства, зафіксовані компанією, зросли на 72% порівняно з 2020 роком і включали крадіжку корпоративних таємниць чи вихідного програмного коду, або навіть змову з іноземними центрами.

Інші інциденти, спричинені інсайдерами, полягали у несанкціонованому або випадковому розкритті інформації (23%), саботажі (19%), шахрайстві (9%).

За підрахунками DTEX, найчастіше інсайдерські інциденти трапляються у фінансовій сфері, на об'єктах критичної інфраструктури та на виробництві (**рис. 2**).

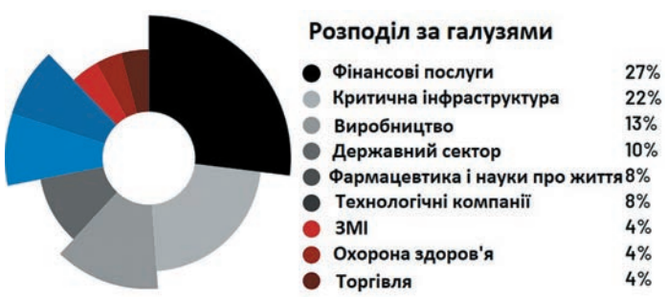

Рис. 2 Статистика інсайдерських інцидентів за різними галузями економіки (джерело: DTEX, 2022 р.)

Карантин і супер-інсайдери

Раджан Ку, комерційний директор DTEX, у статті на сайті VentureBeat пише, що пандемія коронавірусу створила геть нові ризики для фахівців з кібербезпеки, яким зненацька довелося захищати сотні «віддалених офісів» за межами традиційного периметру. У поєднанні з помітним зростанням втоми і масовим звільненням працівників ближче до кінця 2021 року (відомим як «великі відставки» — The Great Resignation) це породило «ідеальний шторм» для інсайдерських загроз.

Пов'язані з цим зміни — наприклад, робота в неурочні години, використання нових програм — призвели до значного зростання аномальної поведінки працівників. У 2020 році DTEX виявила 200% збільшення числа випадків витоку даних через те, що користувачі робили екранні знімки під час спілкування у Microsoft Teams або Zoom, які потім опинялись у ЗМІ або надсилались неавторизованим користувачам. Окрім того, на 300% збільшилась кількість співробітників, які використовували робочі пристрої для особистих цілей, таких як спілкування в соцмережах і онлайн-покупки.

Водночас ця трансформація призвела до постання нового типу кіберзлочинця: зловмисного супер-інсайдера. Це людина, яка володіє серйозними технічними навичками і глибоким знанням поширених методів виявлення саме інсайдерських загроз (часто отриманими безпосередньо на роботі), які дозволяють їй залишатися непоміченою.

Хоча зловмисні супер-інсайдери становлять дуже незначний відсоток усіх користувачів, у третині інцидентів за їхньої участі було застосовано різні просунуті методи. Дослідження DTEX виявило, що 96% супер-інсайдерів спромоглися обійтись без використання атакувальних технік, описаних у базі MITTRE ATT&CK, яка відстежує загальновживані прийоми кіберзлочинців (**рис. 3**).

Рис. 3 Постання зловмисного супер-інсайдера (джерело: DTEX, 2022 р.)

Зловмисні супер-інсайдери намагаються видавати себе за нормальних безневинних користувачів і дотримуються свого звичного графіку роботи. У цьому їм допомагають навички в галузі кібербезпеки загалом і боротьби з витоками даних зокрема, а також знання про побудову кіберзахисту в організації. Також, маючи вже налагоджені

відносини з іншими працівниками, супер-інсайдери мають змогу використовувати більш витончені прийоми соціальної інженерії, ніж фішинг і приманки, якими послуговуються зовнішні злочинці.

Працівники від'їжджають разом з даними

Сайт ***Security Boulevard*** зібрав приклади найгучніших витоків даних з вини інсайдерів. Багато з них були спричинені діями працівників, які саме звільнялися і переходили до конкурентів, забираючи з собою внутрішні конфіденційні файли. Так, у травні 2022 року компанія ***Yahoo*** подала позов проти свого колишнього співробітника на ім'я Цянь Сан, звинувативши його у крадіжці інформації про AdLearn — технологічну платформу для онлайн-замовлень реклами. Цей продукт за допомогою алгоритмів машинного навчання забезпечує адаптивне розміщення реклами у реальному часі відповідно до параметрів, встановлених замовником. Сан очолював одну з чотирьох груп, які займалися розробкою AdLearn.

Як пише сайт ***The Drum***, у лютому Сан отримав вигідну пропозицію щодо працевлаштування від основного конкурента Yahoo в цій галузі — компанії ***The Trade Desk***. Впродовж 45 хвилин після отримання листа — за 4 дні до подання заяви про звільнення — він вивантажив на свої персональні пристрої близько 570 тис. сторінок вихідного коду та іншої інформації, яка стосується AdLearn. За кілька тижнів Yahoo довідалась про крадіжку і офіційним листом наказала Санові надати пристрої для аналізу. Дослідження виявило на носіях «переважну більшість» коду та іншої конфіденційної інформації. «*Присвоєння Саном цих даних позбавило Yahoo ексклюзивного контролю над її корпоративними таємницями*», — вказала компанія в позові, додавши, що крадіжка інтелектуальної власності могла надати перевагу її конкурентам.

Також у квітні ***Apple*** подала до суду на стартап під назвою ***Rivos***, звинувативши його у скоординованому переманюванні співробітників, які працювали над розробкою закритої («пропрієтарної») технології «систем-на-кристалі» (SoC). Rivos найняв 40 інженерів, і принаймні двоє з них, стверджувала Apple, викрали гігабайти конфіденційних даних, які могли «суттєво прискорити» розробку SoC в Rivos. У своєму позові Apple оцінює збитки в мільярди доларів і стверджує, що витратила на розробку технології понад десятиліття, а тепер все опинилося в руках конкурента.

Є в списку є й компанії, які самі спеціалізуються на безпеці інформації. Так, у 2019 році ***McAfee*** звинуватила трьох своїх колишніх співробітників у крадіжці «секретного соусу», тобто інформації про ціноутворення, маркетингових планів, списків клієнтів, методів ведення переговорів та інших чутливих відомостей. Усі троє керували контактами з клієнтами і мали доступ до даних, що вартували десятки мільйонів доларів від продажів. Згідно з позовом, ці працівники впродовж року перейшли до конкуруючої фірми ***Tanium***, прихопивши з собою інформацію.

Побачивши, що в неї переманюють персонал, McAfee провела обстеження комп'ютерів і встановила, що одна з працівниць відправляла сама собі електронною поштою документи, що стосувалися продажів, а інший у свій останній день на роботі відкривав численні конфіденційні файли, при цьому використовуючи неавторизований USB-пристрій. Як зазначив Джефф Стоун, оглядач сайту ***Cyberscoop***, цей випадок підкреслює жорстоку природу індустрії безпеки — відносно невеликої галявини, де фірми весь час конкурують між собою, а працівники часто отримують пропозиції щодо зміни місця роботи.

Подібний випадок стався у компанії ***Proofpoint***, яка в липні 2021 року подала судовий позов проти Семюела Буна, одного зі своїх колишніх директорів, звинувативши його у крадіжці внутрішньої інструкції щодо боротьби на ринку з компанією ***Abnormal Security***. Саме туди у травні того ж року перейшов працювати Бун на посаду директора з продажів. «Перш ніж вийти за двері, Бун поклав до кишені флешку, на яку раніше таємно незаконно записав десятки найсекретніших корпоративних документів Proofpoint, — йдеться в позові. — Потім Бун передав один з ключових документів Abnormal, що забезпечило йому і його новому роботодавцеві несправедливу конкурентну перевагу».

На вимогу Proofpoint Бун повернув носій, проте в компанії зазначили: нема жодного практичного способу встановити, що він не зробив собі інші копії і що не передав Abnormal ще якісь документи окрім тих, які визнав. Сайт ***CRN.com*** додає, що Бун здогадно завантажив і іншу чутливу інформацію, зокрема пропозиції торговим партнерам, списки облікових записів кінцевих користувачів і квартальні звіти. За даними Proofpoint, принаймні ще двоє колишніх співробітників, які перейшли до Abnormal, незаконно завантажували корпоративні файли. Іронія в тому, що Proofpoint, зокрема, пропонує системи для захисту від витоків даних — її власне DLP-рішення не завадило працівникам скопіювати і забрати з собою важливі документи.

В інших випадках витоки сталися не зі злого умислу, а через звичайне недбальство. У 2017 році один зі співробітників ***Boeing*** відправив файл Excel своїй дружині, яка не була працівницею компанії, щоб та допомогла його відформатувати. Документ містив персональні дані 36 тис. співробітників Boeing, у тому числі дати народження і номери соціального страхування, які знаходились у прихованих колонках. Компанія дізналась про цей випадок більш ніж через 6 тижнів і провела обстеження комп'ютерів винуватця і його дружини. Хоча Boeing стверджує, що усі копії документа було видалено і він не поширився за межі цих двох пристроїв, вона запропонувала усім співробітникам безкоштовний дворічний моніторинг кредитних історій.

У серпні вже нинішнього року декілька співробітників ***Microsoft*** вивантажили свої логіни і паролі

в інфраструктуру GitHub. Вона належить самій Microsoft, проте ця інформація потенційно могла надати будь-кому, зокрема й хакерам, доступ до серверів Azure і потенційно до інших внутрішніх систем. Хоча Microsoft не розкрила, які саме ресурси були захищені цими паролями, у разі, якби зловмисники отримали доступ до інформації про користувачів з країн ЄС, Microsoft загрожував би штраф у розмірі до €20 млн відповідно до регламенту GDPR. На щастя, виток завчасно помітила компанія зі сфери кібербезпеки ***spiderSilk***, яка повідомила про це Miscrosoft. Там провели розслідування і не виявили, щоб хтось дістався до чутливих даних, і вживають заходів для недопущення повторення такої ситуації.

Штраф у розмірі £18,4 млн довелося сплатити в 2020 році готельній мережі ***Mariott*** за відомий витік персональних даних 339 млн гостей у 2018 році. Проте на цьому прикрощі компанії не скінчилися. Того-таки 2020 року хакери вкрали персональні дані 5,2 млн гостей британських готелів. Вони скористалися вкраденими обліковими записами двох працівників іншої компанії, яка працювала під брендом Mariott, і отримали доступ до програми управління готелем. Вже у 2022 році був ще один інцидент, цього разу в США, коли за допомогою соціальної інженерії хакери спонукали одного працівника відкрити доступ до свого комп'ютера, проте Mariott стверджує, що вкрадено було в основному несекретні дані, які стосувалися внутрішньої діяльності компанії.

Інсайдерам бій

Gartner визначає управління ризиками, пов'язаними з інсайдерами (Insider Risk Management — IRM) як інструменти та можливості для оцінювання, виявлення та ізоляції небажаної поведінки довірених облікових записів усередині організації. Архітектура зменшення ризиків, що її пропонує Gartner, складається з трьох шарів, а саме сенсорів, аналізу й реагування. Зокрема, до шару сенсорів входять системи запобігання витокам (DLP), системи керування інформаційною безпекою та подіями (SIEM), системи управління обліковими записами (IAM), а також пастки і засоби для моніторингу.

Gartner зазначає: IRM суттєво відрізняється від традиційних засобів протистояння атакам тим, що інсайдери користуються довірою всередині організації. При цьому понад 50% інцидентів не пов'язані зі злим умислом, через що звичні методи виявлення та знешкодження загроз недоцільно застосовувати. А також, хоча хакери зазвичай намагаються проникнути в організацію і набути привілеїв у мережі, набагато частіше своїми привілеями зловживають самі співробітники, будь то з поганими намірами чи без.

Важливо, що інсайдерські загрози не обмежуються крадіжкою даних; так само серйозною є проблема, коли нові працівники приносять з собою інтелектуальну власність зі свого попереднього місця роботи. Це може призвести до «заплямування» продукту і потенційних судових позовів. Що, власне, й видно з прикладів, наведених у попередньому розділі.

Продукти і сервіси IRM забезпечують можливості моніторингу і спостереження; під першим мається на увазі контроль даних, а під другим — стеження (відкрите чи приховане) за діяльністю конкретних працівників. Інструменти спостереження контролюють переписку електронною поштою, дії в Інтернеті (відвідувані веб-сторінки, проведений на них час тощо), онлайн-пошук, месенджери, операції з файлами тощо. Додаткову інформацію надають засоби моніторингу соціальних мереж (наприклад, для контролю персоналу, який використовує цей канал комунікації для продажів), брокери доступу до хмарних сервісів CASB, системи уніфікованого управління терміналами UEM для контролю інформації як на ПК, так і на мобільних пристроях.

Тут знову-таки можна послатися на дослідження Ponemon Institute, згідно з яким найбільш популярними технологіями, які використовують для зменшення збитків від інсайдерських атак, є DLP і системи управління привілеями доступу (PAM) — їх назвали відповідно 64% і 60% респондентів. 57% використовують системи аналізу поведінки користувачів і сутностей (UEBA), 50% — системи виявлення і знешкодження загроз на кінцевих точках (EDR), і 41% організацій вказали загалом рішення з управління ризиками інсайдерських атак.

Далі розповімо про кілька прикладів технічних рішень, які забезпечують захист від інсайдерських загроз.

Fortinet у цьому напрямку пропонує своє рішення ***FortiInsight***. Ця система, яка належить до класу UEBA, інтегрована в загальну інфраструктуру безпеки Fortinet Security Fabric. FortiInsight збирає дані з машин користувачів за допомогою «розумних конекторів» — агентів, які, за твердженням виробника, споживають менш ніж 0,5% потужності CPU, 20 МБ оперативної пам'яті і 5 кбіт/с трафіка. Дані від агентів передаються у форматі, який відповідає «5-факторній моделі», тобто містять ідентифікатор машини, ім'я користувача та назву програми, тип дії і ресурс, з яким цю дію було вчинено (наприклад, копіювання файлу на знімний носій).

Механізм на основі машинного навчання, який лежить в основі FortiInsight, автоматично визначає нормальну поведінку користувачів, і надалі агенти в реальному часі надсилають інформацію про виявлені аномалії в цій поведінці. Аномалії потім перевіряються на наявність факторів ризику, такі як використання знімних носіїв чи хакерських інструментів, доступ до файлів, який становить порушення заданої політики. Результат поєднується з даними про попередні реакції на такі дії, і факторові присвоюється загальний бал ризику. Про дії, які FortiInsight вважає ризикованими, одразу сповіщається команда кібербезпеки.

FortiInsight пропонується як хмарне рішення (SaaS-послуга, яку надає Fortinet), а також для локального розміщення у замовника на віртуальних машинах або ж як частина рішення FortiSIEM.

Також рішення UEBA для захисту від інсайдерських загроз пропонує компанія ***Exabeam***. Ця система визначає інсайдерські загрози у чотири кроки. Процедура починається з отримання початкових відомостей, таких як дані про реєстрацію від SIEM або хмарних сервісів, дані про користувачів з Active Directory, результати сканування DLP, додаткова інформація Threat Intelligence тощо. Базові дані про подію можуть містити лише мінімальну ідентифікувальну інформацію — наприклад, IP-адресу, — але вони автоматично збагачуються іншими контекстуальними відомостями.

Далі процес під назвою Smart Timelines «зшиває» історію дій користувача з урахуванням різних задіяних облікових записів, пристроїв та ресурсів. Це дозволяє виявляти комплексні спроби доступу до даних і надає персоналу з кібербезпеки повну історію атаки. На третьому етапі механізм поведінкового аналізу створює шаблони нормальної поведінки для кожного користувача та ресурсу, а на четвертому дані Smart Timelines порівнюються з шаблонами і генерується чітка картина ризику потенційного витоку даних.

Для оцінювання інсайдерських загроз Exabeam використовує різні технології на основі машинного навчання, як-от: побудова шаблонів поведінки, груповий аналіз (порівняння поведінки і патернів доступу користувача з діями колег), аналіз привілейованих облікових записів, аналіз спільних облікових записів з атрибуцією дій усіх співробітників, які ними користуються, а також аналіз заблокованих облікових записів (наприклад, пов'язаних з попередньою посадою співробітника). Ідентифікувавши користувачів, які поводяться аномально, Exabeam може вживати заходів різного рівня строгості: наприклад, поінформувати аналітика, надіслати працівникові листа з нагадуванням про необхідність дотримуватися правил конфіденційності, або взагалі заблокувати доступ. Користувачі системи можуть створювати власні правила реагування на події.

Американська компанія ***Netwrix*** спеціалізується на продуктах у царині захисту даних, найвідомішим з яких є ***Netwrix Auditor***. Ця система, як видно з назви, взагалі-то призначена для аудиту IT-інфраструктури з метою вдосконалення захисту, проте вона помічна при виявленні ризиків і контролі діяльності співробітників.

Netwrix Auditor генерує сповіщення і звіти для різних небезпечних ситуацій. Наприклад, він попереджає про нетипові спроби доступу до даних, тобто коли хтось відкриває файли, яких майже ніколи раніше не відкривав (за умовчанням не більше двох разів). У звіті також висвітлюються користувачі, які за відносно короткий проміжок (за умовчанням тиждень) здійснили більше дій, ніж за порівняно довший (30 днів). Є звіт, який фіксує дані про діяльність користувачів у неробочі години.

Ще один звіт показує, коли користувач заходив у свій обліковий запис на різних робочих станціях протягом короткого проміжку часу — це може свідчити про те, що пароль вкрадено або скомпрометовано. Є можливість контролювати тимчасові облікові записи, тобто такі, які було видалено невдовзі після створення: звіт містить дані про те, хто і коли створював і знищував такі облікові записи. З їх допомогою злочинці можуть приховати свою діяльність.

Якщо користувачі створюють файли, з назви яких видно, що там міститься чутлива інформація, це теж відображається у звітах. Система за замовчанням ідентифікує файли, що містять слова на кшталт «пароль», «карта», «платіж», «власник» тощо. Система попереджає про створення, модифікацію або видалення потенційно небезпечних файлів, таких як інсталятори, скрипти і ключі реєстру у спільних папках та на сайтах Microsoft SharePoint. Ці файли можуть бути шкідливими програмами або небажаними дистрибутивами, які можуть призводити до інцидентів безпеки.

Колектив проти інсайдерів

Втім, спеціалісти з кібербезпеки кажуть, що боротьба з інсайдерськими загрозами — це річ комплексна, яка не обмежується технологіями. Раджан Ку з DTEX Systems зазначає, що протистояння інсайдерам вимагає розуміння людської поведінки, психосоціальних чинників і трендів, а також нюху на аномалії. Воно потребує взаємодії між різними підрозділами: HR, фінансовим, юридичним, технічним і кібербезпеки. Тому краще мати програму боротьби з інсайдерськими ризиками окремо від центру управління кібербезпекою (SOC), призначенням якого є виявлення і знешкодження зовнішніх загроз, стверджує Ку.

Як вказує Exabeam на своєму сайті, є чимало історій про те, як HR-відділ не повідомляв групу IT-безпеки про звільнення співробітників. Координація між начальником відділу кадрів і шефом «безпечників» буде помічною, адже якщо просто занести відповідних співробітників у список спостереження, це може відвернути багато загроз. HR також може, наприклад, повідомляти про співробітників, які не отримали підвищення або яким не збільшили зарплатню. З інших організаційних заходів Exabeam рекомендує навчати персонал протидіяти фішингу і доповідати про чиюсь підозрілу поведінку, а також радить мати виділений персонал, який стежить за такими проявами.

Gartner рекомендує прописати внутрішню політику безпеки, яка регламентує використання засобів спостереження і моніторингу, термін зберігання зібраних даних, хто має право ініціювати спостереження і мати доступ до його результатів. З іншого боку, потрібно чітко задокументувати, які дії при користуванні інфраструктурою компанії є заборонені або їх потрібно уникати.

Це досить серйозний комплекс заходів, яких, однак, доведеться вживати, щоб забезпечити баланс між захистом корпоративних таємниць і правом співробітників на конфіденційність.

Василь ТКАЧЕНКО, **«МтБ»**