

ІНФОРМАЦІЙНА БЕЗПЕКА: ВАЖЛИВО, ВІДПОВІДАЛЬНО, УСПІШНО. КЕЙС-ІНТЕРВ'Ю ПРО ДОСВІД СТВОРЕННЯ СИСТЕМИ ІБ НА БАЗІ MCAfee ENTERPRISE

Протистояти сучасним загрозам може лише комплексна безпека. Компанії часто не знають, як збудувати таку безпеку. У них виникає безліч питань: «З чого почати?», «Які можуть виникнути труднощі?», «Чи може комплексна безпека коштувати недорого?» Щоб дізнатися, як забезпечує інформаційну безпеку компанія з різними бізнесовими напрямками, ми взяли інтерв'ю у Андрія Кононцова — начальника відділу інформаційної безпеки МТІ ГРУП.

Група компаній МТІ — це диверсифікований бізнес, який об'єднує три базові напрямки:

- Інформаційно-комунікаційні технології, такі як дистрибуція, гарантійний та післягарантійний сервіс, проєктування і впровадження систем безпеки (антикравдіжних систем, систем контролю доступу, управління складом на базі RFID-технології)
- Роздрібна торгівля (взуття, одяг, ювелірні прикраси, електроніка)
- 3-PL оператор (послуги зі зберігання, обробки та доставки вантажів).

■ Андрію, наскільки складно забезпечувати безпеку в такій великій компанії?

Така роздробленість та неоднорідність напрямків нашого бізнесу дуже позначається на вимогах до безпеки. Вибираючи будь-які рішення для ІБ або ІТ, ми обов'язково маємо враховувати не лише завдання конкретної компанії холдингу, а ще й її місце у загальній інфраструктурі. Наприклад, захист кінцевих точок має однаково добре працювати на комп'ютері як менеджера роздрібного магазину, так і Sales Manager'а ІТ-дистриб'ютора, бухгалтерів, ІТ-співробітників чи керівників. Комп'ютерна техніка, використовуване ПЗ та знання в ІТ сфері різні, а справлятися з усім має єдина система безпеки. Тим паче, що типи загроз, частота атак та їх специфіка є багатоманітними.

■ Які відділи займаються безпекою?

Безпека — це цілий окремий кластер у структурі компанії, завдання якого в напрямку кібербезпеки хоч і перегукуються із завданнями ІТ-відділу, але здебільшого все ж таки відрізняються як у технічному плані, так і в самій суті. Раніше захистом кінцевих точок та мережі займався ІТ-підрозділ.

«Зі зростанням загроз, появою нових рішень та аналізу ризиків ІБ ми зрозуміли, що для оперативного реагування на сучасні кіберзагрози потрібно займатися безпекою не за залишковим принципом, а насамперед. Та й по суті, на ІТ лежать питання підтримки інфраструктури, щоб все працювало, вчасно лагодилося і т.д. Тому ми вирішили провести невелику реформу та перемістити всю технічну безпеку до відділу інформаційної безпеки.»

■ Нещодавно ви впровадили рішення для захисту даних у хмарі (CASB) та виявлення загроз на кінцевих точках та реагування на них (EDR). Розкажіть, як дійшли необхідності цих рішень?

Ми досить довго йшли до тієї інфраструктури, яку маємо зараз. Спочатку це були спроби роботи з хмарними ресурсами, потім повальна міграція сервісів у хмару. З переходом у хмару ми мали терміново розібратися, як забезпечувати якісний захист та розуміти, що відбувається з нашими даними. Насамперед цей запит надійшов від бізнесу, для підвищення гнучкості та оптимізації бізнес-процесів. Перед нами гостро постало питання – як забезпечити безпеку даних у хмарах в тому числі для сервісів Office 365, контроль переміщення даних та розмежування доступу, де б не знаходилися користувач та пристрій (на роботі чи вдома). Вирішили не формувати розрізнену інфраструктуру безпеки, оскільки для її супроводу потрібно більше ресурсів і, насамперед, більше фахівців. Тому спочатку, проаналізувавши рішення кількох виробників, вирішили будувати безпеку на продуктах McAfee. Відповідно, масштабувати безпеку також вирішили з використанням продуктів цього виробника. Так у нас з'явився весь антивірусний комплекс із захисту кінцевих точок. Пізніше, як я вже казав, ми почали активно використовувати хмарні послуги, і тому нам знадобився брокер безпечного доступу до хмар. CASB від McAfee — це лідер у даному класі рішень, що тоді, що зараз.

Але антивірусний захист на землі та у хмарі — це лише частина безпеки. Складність та кількість векторів атак значно зросла за останній час. Для нас стало очевидним, що рішення захисту, хай навіть «просунутий антивірус», не можуть дати повної видимості того, що у нас відбувається в мережі та на кінцевих точках. За допомогою нього не можна побудувати форензику та повноцінно розслідувати інциденти ІБ. І воно по суті для цього і не призначено. Тому ми вирішили впровадити EDR. З таким набором інструментів ми були готові до всього, і пандемія не застала нас зненацька. Протягом одного дня ми змогли перейти на віддалений режим роботи.

■ Які критерії були важливими при виборі CASB та EDR?

На нашому ринку все ж таки перше місце займає ціна — багато компаній не можуть дозволити собі колосальних витрат на безпеку, а тому іноді змушені йти на компроміси у вигляді опенсорсних рішень. У нас теж не було повної фінансової свободи, але бюджет дозволяв обрати рішення у кращому співвідношенні ціна/якість. Продукти McAfee завжди знаходяться в лідерах на ринку і часто виявляються значно доступнішими за конкурентів.

Наступний критерій – можливість інтеграції з іншими компонентами інфраструктури. Без такої гнучкості безпека буде не єдиною логічною системою, а просто незв'язаним набором інструментів, що, певна річ, знижує ефективність безпеки в цілому. Інтеграція рішень «з коробки», у разі McAfee, не тільки прискорює виявлення складних загроз, але й дає можливість автоматизації для швидкого реагування на них.

Замикає трійку, зрозуміло, функціонал самого продукту. Одним з головних завдань у нас є контроль та захист даних у хмарах. Пілот рішення CASB від McAfee показав, що продукт має широкий функціонал і, що важливо, зручний інтерфейс. Яскравий приклад використання – це Office 365. Також нас приваблювало те, що рішення є абсолютним лідером за результатами оцінки Gartner.

■ Якими були альтернативні варіанти рішень безпеки?

На перший погляд, альтернатив здавалося багато. Потім, коли почали заглиблюватися в рішення інших виробників, виявилось, що багато продуктів ще не такі «зрілі». Зараз багато виробників розширюють свої продуктові лінійки, але їхні продукти на етапі виведення на ринок можуть мати досить низьку і привабливу вартість. А ось їхні можливості далеко не завжди вирішують актуальні завдання безпеки. З етичних норм не буду називати назви компаній.

Ми зупинилися на 2–3 виробниках. Зваживши всі фактори після проведення пілота, ми вибрали рішення McAfee. Одним з важливих факторів було те, що McAfee має досить сильні рішення як для захисту кінцевих точок, так і для захисту хмари. До того ж, вся система вже спиралася на McAfee і ми вирішили не витрачати час та кошти на перенавчання фахівців без вагомих переваг.

■ Як пройшло впровадження рішень?

З впровадженням CASB, EDR та інших продуктів вендора жодних проблем не було. Щодо CASB зазначу, що велику роль відіграє докладна і зрозуміла документація — всі налаштування, схеми та варіанти інтеграцій вже надані «з коробки». Рішення CASB та EDR постачаються як SaaS і не вимагають встановлення серверної інфраструктури. Я сам усе інтегрував без додаткових навчань і створював початкові політики. Там немає якихось серйозних складнощів.

Потішило те, що всі наші напрацювання з пілотної версії перейшли до платної ліцензії, тож нам не довелося починати з нуля.

■ До речі, чи легко управляти одразу всіма системами безпеки?

Зручне управління, напевно, один із тих критеріїв, на яких базувався наш вибір. У McAfee це вирішується за допомогою ePolicy Orchestrator – єдиної консолі для управління всіма рішеннями безпеки. Оскільки для нас є актуальним завдання впоратися з різними рішеннями для захисту інфраструктур неоднорідних компаній, така оркестрація стає обов'язковою. Управління з єдиної точки ми давно визначили як критерій відбору будь-якого захисту.

■ Що ви особисто відзначили в продуктах McAfee?

Впроваджуючи CASB, ми потребували брокера безпечного доступу до хмар і більш детального контролю в O365 за помірні витрати. Іноді впровадження чогось нового додає нових проблем із продуктивністю та дає навантаження на систему. Як результат – ІБ та ІТ починають конфліктувати та з'ясовувати пріоритети. Але McAfee не навантажує інфраструктуру та дозволяє всім спокійно працювати.

Рішення CASB зручне, оскільки політики швидко та легко налаштовуються, їх можна підігнати під себе до дрібниць, підв'язати пристрої тощо. Іншими словами, це не забирає багато часу. Зрозуміло, ідеальних систем не існує, і бувають профілактики, оновлення та якісь нюанси. Але головне – проблеми трапляються нечасто, а вендор швидко на них реагує. Щодо рішення EDR скажу, що воно дуже розширює можливості захисту та дійсно допомагає в роботі. EDR значно підвищує видимість того, що відбувається, підвищує можливості для оперативного блокування процесів або переміщення до «карантину» ураженої робочої станції, спрощує визначення зв'язків між подіями безпеки та дає можливість швидко вживати заходів.

■ Які інші інструменти McAfee ви використовуєте?

McAfee має MVISION Insights, який у нас теж включений у функціонал. Хоча, на перший погляд, це досить факультативне рішення (воно безпосередньо нічого не захищає і не блокує), практичної користі від нього значно більше, ніж може здатися. Я б сказав, що це рішення стосується проактивного захисту. По-перше, MVISION Insights перевіряє вас ще раз, тобто, по суті проводить аудит політик безпеки. Якщо фахівець забув активувати якусь функцію, безпекову політику або десь не встановив продукт, критично важливий для відбиття атак — рішення це помітить і сповістить його.

По-друге, воно замінює купу підписок на різні новини та інші ресурси. Ви дізнаєтесь, як змінюється ландшафт загроз у світі, в Україні, за напрямками бізнесів. Ви отримаєте повну інформацію про їх маркери компрометації, цілі атак, а також дані від інших вендорів по цим атакам. У самому рішенні ви зможете порівняти отриману інформацію з MITRE ATT&CK та оцінити, яка з атак є потенційною загрозою для вашої компанії.

■ Що ви можете загалом сказати про комплекс рішень з безпеки від McAfee?

Я назвав би рішення McAfee конструктором, де багато залежить від самих фахівців і того, як вони спроєктують захист. У цьому сенсі архітектура рішень та підходи – це фундамент, на якому будується безпека. Спочатку ми для себе відзначили, що з платформою безпеки та підходами McAfee ми зможемо забезпечити інтеграцію рішень, а отже, і автоматизацію з реагування на атаки. На етапі, коли ми визначали стратегію розвитку безпеки, ми вирішили, що для нас це важливо. Якщо до цього питання спочатку не підійти системно, можна отримати «зоопарк» з різних рішень, а разом з тим – непов'язану та неефективну інфраструктуру безпеки.

На базі продуктів McAfee можна будувати ешелонований захист на різних рівнях, при цьому зручно управляти і все налаштовувати з однієї консолі. У рішень є синергія. При цьому окремі продукти теж досить ефективні, тому вирішити можна абсолютно будь-які завдання безпеки.

Наразі ми вже маємо комплекс безпеки. Але ми бачимо, що нам не вистачає Пісочниці та SIEM, тож розмірковуємо над їх придбанням. Я радий, що керівництво з розумінням ставиться до наших ініціатив та проєктів щодо розвитку ІБ, адже від безпеки насамперед залежить стабільність бізнес-процесів.



Андрій Кононцев
Начальник відділу інформаційної безпеки МТІ ГРУП