Концепція Сучасної Архітектури Менеджменту Процесів Інформаційної Безпеки Soapa

Копиченко Іван
начальник відділу технічного захисту інформації
КП «Обласний інформаційно-аналітичній центр»
Одесса, Україна
ikopychenko@odessa.gov.ua

The Concept of Modern Information Security Processes Management Architecture Soapa

Kopychenko Ivan
head of Technical Information protection department
Municipal Enterprise. Regional Information and Analytical Center
Odessa, Ukraine
ikopychenko@odessa.gov.ua

***Анотація*—Безперервне збільшення інформаційних і телекомунікаційних систем мережевої інфраструктури компаній, так саме як і значне збільшення обсягів телеметричної інформації, що генерується такими системами, вимагає впровадження більш розвинених моделей управління подіями інформаційної безпеки. Саме через це фахівцями ESG (Enterprise strategy group) було запропоновано нову програмну архітектуру SOAPA.**

***Abstract*—The continuous increase in information and telecommunications systems of the company's network infrastructure, as well as a significant increase in the volumes of telemetric information generated by such systems, requires the introduction of more advanced models of information security event management. That is why the specialists of the Enterprise strategy group proposed a new software architecture called SOAPA.**

Ключові слова—безпека; SIEM; СУІБ; кібербезпека; архітектура; аналітика; управління; мережа; захист; автоматизація

Keywords—security; SIEM; ISMS; cybersecurity; architecture; analytics; management; network; defense; automation

I. Вступ

У сучасних реаліях забезпечення інформаційної безпеки перестало сприйматися як технічна задача, а стала серйозною бізнес проблемою для багатьох підприємств стурбованих своєю репутацією і місцем на ринку. Для забезпечення безпеки даних, які обробляються за допомогою інформаційно-телекомунікаційних систем підприємства, недостатньо лише побудувати надійну систему захисту інформації, а й вкрай важливо забезпечити її постійну підтримку, розвиток і управління протягом усього життєвого циклу.

Для вирішення саме такого завдання фахівцями ESG була запропонована концепція нової архітектури менеджменту процесів інформаційної безпеки SOAPA (security operations and analytics platform architecture). Дана архітектура стала неминучим кроком у розвитку SIEM (Security information and event management) систем.

Фахівці із інформаційної безпеки та інсайдери стверджують, що 2017 рік стане важким роком, наповненим атаками на державні ресурси, вірусною активністю та витоками даних. В першу чергу це пов’язано із тенденціями розвитку інформаційних технологій, які в значній мірі ускладнюють забезпечення інформаційної безпеки:

Хмарні сервіси. Все більше систем та інформаційних навантажень переносять в приватні та публічні хмарні сервіси.

Інтернет речей. Згідно із прогнозами, до 2020 року очікується більш ніж 20 мільярдів підключених до мережі Інтернет пристроїв. Вже сьогодні сфери діяльності пов’язані із енергетикою, охороною здоров’я та промисловістю активно впроваджують IoT (internet of things) пристрої.

Зростання мережі. Фізичні мережі і мережеві магістралі розширюються від 10Гб до 40 / 100Gb, продовжується перехід від IPv4 до IPv6. Все це призводить до збільшення об’ємів трафіку, сеансів,

пакетів, потоків та протоколів, за якими необхідно стежити.

Перенесення робочих процесів в електронні системи. Велика кількість державних та приватних установ автоматизують робочі процеси та переносять роботу в електронні системи.

II. Призначення архітектури

В процесі управлінні інформаційною безпекою дуже важливо не губитися в великих обсягах інформації, що генерується системами управління інформаційною безпекою (СУІБ). Навіть якщо всередині підприємства існує центр управління інформаційною безпекою (security operations center - SOC), фахівець часто не здатний впоратися з обробкою всіх даних, що надходять.

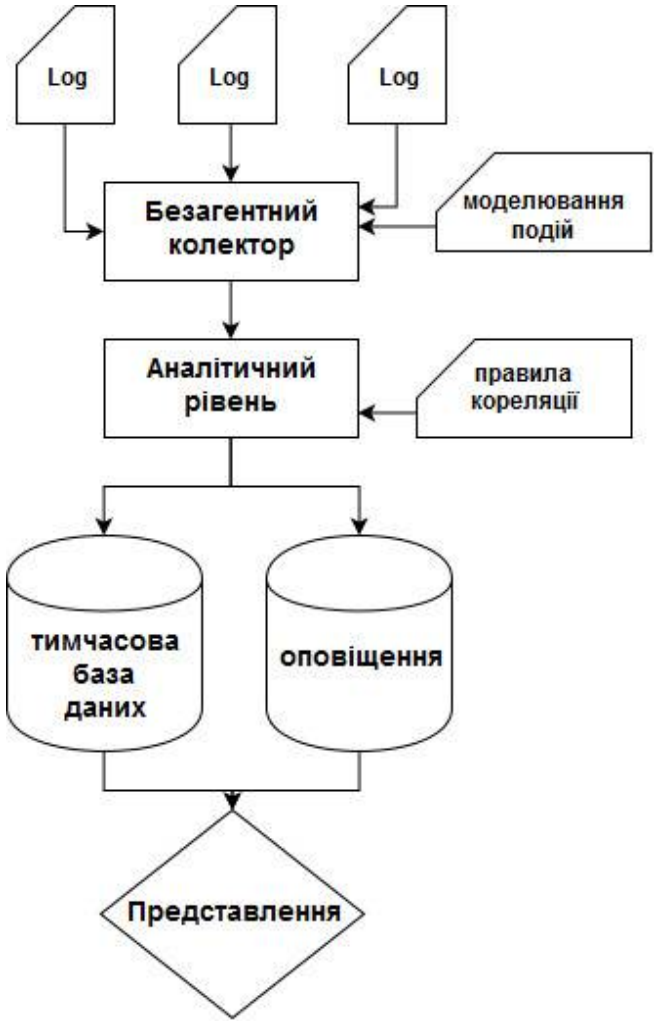

Рис. 1. Типовий схема взаємодії вузлів SIEM системи

Рішенням такої проблеми для підприємства може стати впровадження системи, побудованої на базі архітектури SOAPA, яка дозволяє підвищити ефективність роботи фахівців з інформаційної безпеки, в умовах значного нарощування обсягів внутрішньої інформаційно-телекомунікаційної структури підприємства.

На сьогодні основною категорією споживачів таких систем є підприємства, що працюють в банківській сфері. Адже саме їм необхідно регулярно проводити зовнішні аудиторські перевірки на відповідність. У банківській сфері здійснюється обробка великої кількості чутливої інформації, тому в разі виникнення інцидентів стає критично важливим володіння інформацією про те, хто/коли/звідки допустив витік, чи було це зловмисною дію або випадковою, а також наявність та характеристика супутніх факторів.

Так само потреба в SOAPA виникає у приватних підприємств з великим географічним розподілом. У таких підприємств часто виникають проблеми усереднення даних. Замість того щоб дивитися на проблему комплексно, події розглядаються в потоці загальної інформації, і часто залишаються без належної уваги через низький пріоритету окремих показників.

Нарешті, SOAPA може стати наступним кроком розвитку інформаційної безпеки для підприємств, у яких вже побудована повноцінна система управління подіями інформаційної безпеки, але існує потреба в поліпшенні процесу запобігання та захисту від атак.

Основна перевага SOAPA перед іншими архітектурами полягає в тому, що вона дозволяє не тільки аналізувати події, створювати красиві звіти і управляти ризиками, а й автоматизовано управляти ролями користувачів системи, розмежовувати права доступу, відстежувати аномалії поведінки користувача та трафіку всередині мережі, аналізувати вхідні дані на уразливості та, що найважливіше - об'єднати всі розрізнені системи інформаційної безпеки в один комплексний механізм.

Дана архітектура дозволяє підтримувати взаємодію підсистем за допомогою великого числа протоколів і інтерфейсів:

Syslog

SNMPv2 SNMPv3

HTTP, HTTPS

SQL

WMI

FTP SFTP

SSH

Rsync

SAMBA

Однак, слід також зазначити, що впровадження подібних систем без попереднього аналізу та підготовчих робіт може привести не тільки до нераціонального використання виділених ресурсів і надлишковості в роботі системи, але і до отримання абсолютно зворотного ефекту, очікуваного від системи, а саме значного збільшення ризиків пов'язаних з інформаційною безпекою підприємства.

Перш ніж впроваджувати системи менеджменту інформаційної безпеки, керівництву, спільно з фахівцями з інформаційної безпеки, в обов'язковому порядку необхідно провести ряд підготовчих робіт, а саме:

визначення області дії СУІБ

збір вихідних даних про бізнес-процеси, структурні підрозділи, інфраструктуру, методи і засоби забезпечення інформаційної безпеки.

аналіз діючої організаційно-розпорядчої документації, що регламентує питання забезпечення інформаційної безпеки

проведення оцінки ризиків:

інвентаризація та класифікація активів;

формування карти загроз;

розробка процесів управління інформаційною безпекою;

розробка процесів забезпечення інформаційної безпеки;

розробка комплекту організаційно-розпорядчої документації, що регламентує питання забезпечення інформаційної безпеки;

впровадження процедур і документації СУІБ:

впровадження процесів управління інформаційною безпекою;

впровадження процесів забезпечення інформаційної безпеки;

впровадження системи обробки подій та журналів.

III. Елементи архітектури

Дуже часто, у випадках коли у підприємства виникає питання автоматизації роботи своєї системи управління інформаційною безпекою, стає очевидною недостатність функціоналу звичних рішень. SOAPA розвивається як динамічна архітектура, і це значить що в майбутньому в неї можуть бути інтегровані нові системи. На сьогодні до складу архітектури SOAPA входять:

інструменти виявлення/реагування на кінцевих вузлах (EDR)—часто аналітику інформаційної безпеки підприємства необхідно поглибитися в оповіщення про тривогу спостерігаючи за користувачем системи та досліджуючи його поведінку

платформи реагування на інциденти (IRPs)—крім збору, обробки та аналізу даних, фахівцю з безпеки важливо якомога швидше сповіщати про проблеми безпеки та виправляти їх

системи аналітики мережевої безпеки—доповнює системи виявлення та реагування на загрози аналізом на рівні аналізу потоку пакетів

системи аналітики поведінки користувача/алгоритми машинного навчання (UBA|MLA)—автоматизує обробку великих обсягів інформації

сканери уразливостей та засоби керування безпекою—допомагає спеціалісту із безпеки встановлювати пріоритети аналізу та управління уразливостями

пісочниці для запобігання шкідливому програмному забезпеченню (anti-malware sandboxes)— дозволяє проводити ручний або автоматизований аналіз та зворотній інжиніринг можливих заражених файлів, а також пошук уразливостей нульового дня (0-day)

системи розвідки загроз— для організацій дуже важливо проводити порівняння внутрішніх аномалій із відомими та задокументованими уразливостями. Також необхідно створювати та наповнювати загальнодоступні джерела таких загроз

Керуючись схемою типового життєвого циклу хакерської атаки на інформаційні ресурси підприємства, яка наведена на рис. 1, можна побачити, що такий тип архітектури системи менеджменту процесів інформаційної безпеки дозволяє не тільки детектувати та передбачати атаку, але й автоматично запобігати їй ще на рівні системи управління інформаційною безпекою. Спираючись на метод статистичного модулювання, система має можливість автоматично ідентифікувати незвичайну поведінку, пов’язану із хакерською атакою. Далі, використовуючи процес машинного самонавчання, вона може самостійно відрізняти «нормальне» від «аномального».

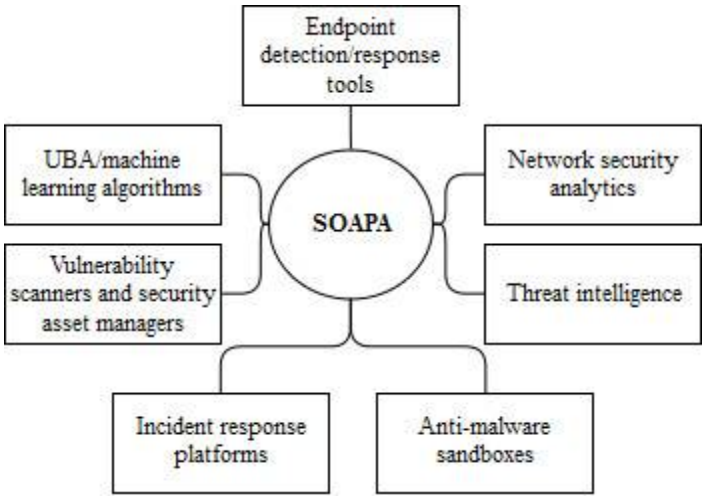

Рис. 2. Елементи, що входять в склад архітектури SOAPA

Збір інформації		
Тип атаки	***Цілі***	***Засоби***
Дослідження відкритої інформації	- веб сервери - зовнішні додатки - соціальні медіа	- пошукові сервіси - публічна інформація - зовнішнє сканування
Первісна експлуатація		

Тип атаки	*Цілі*	*Засоби*
Ініціювання атаки	- керівництво та фахівці - віддаленні співробітники	- вразливості нульового дня - соціальна інженерія - фішинг - створення дір
Створення пладарму	- робочі станції - web-сервери	- встановлене шкідливе ПЗ - вкрадені облікові записи

Управління та контроль		
Тип атаки	*Цілі*	*Засоби*
Отримання доступу	- системи безпеки - операційні системи	- руткіти - трояни - створення облікових записів - створення VPN
Внутрішня розвідка	- спільні каталоги - робочі станції - сервери - маршрутизатори	- встановлене шкідливе ПЗ - вкрадені облікові записи

Підвищення привілеїв		
Тип атаки	*Цілі*	*Засоби*
Горизонтальне переміщення	- спільні каталоги - робочі станції - сервери - маршрутизатори	- віддалене управління - вкрадені облікові записи
Підвищення привілеїв	- облікові записи адміністраторів - сервери - маршрутизатори	- руткіти - трояни - створення облікових записів

Управління даними		
Тип атаки	*Цілі*	*Засоби*
Збір та шифрування даних	- спільні каталоги - робочі станції - сервери - документи	- ftp або email - ZIP & RAR компресія - криптолокери
Викрадення даних	- документи - дослідження і розробки	- ftp або email - веб-розміщення - шифровані тунелі

Рис. 3. Типовий життєвий цикл хакерської атаки на інформаційні ресурси підприємства.

IV. Висновки

Архітектура SOAPA дозволяє більш поглиблено автоматизувати менеджмент процесів інформаційної безпеки підприємства в умовах значного збільшення обсягів даних, що генеруються системою управління інформаційною безпекою. Така архітектура дозволяє значно спростити життя фахівцям, і допомагає розставити пріоритети реагування на інциденти. Але однією з основних причин розробки нової архітектури стала не тільки необхідність автоматизації обробки інформації, а й автоматичне реагування на зовнішні і внутрішні загрози інформаційним ресурсам підприємства.

Слід також окремо відзначити, що доцільність та ефективність можливості впровадження SOAPA в державному секторі доки що не визначено. Але доцільність використання в банківській сфері не викликає сумнівів, так як вона підпорядковується міжнародним стандартам, і не суперечить існуючому законодавству в сфері захисту інформації в Україні. Так само варто пам'ятати що це всього лише концепція, і в найближчому майбутньому в неї можуть бути додані нові підсистеми.

Перевагами даної концепції є динамічність та швидка адаптованість умов інформаційно-комунікаційної архітектури.

Література References

[1] David R. Miller, Shon Harris, Stephen Vandyke, Security Information and Event Management (SIEM) implementation, McGrawHill, 2011.

[2] ISO/IEC27000 seriesFAQ–ISO27kForum[Електронний ресурс]. – Режим доступу: http://www.iso27001security.com/ html/faq.html.

[3] J. Oltsik, Security: Goodbye SIEM, Hello SOAPA?[Електронний ресурс]. – Режим доступу: https://www.channele2e.com/2016/12/28/security-goodbye-siem-hello-soapa

[4] J. Oltsik, Security: Security data growth drives SOAPA [Електронний ресурс]. – Режим доступу: http://www.networkworld.com/article/3154090/security/security-data-growth-drives-security-operations-and-analytics-platform-architecture-soapa.html

[5] O. Salah, Mandatory Information Security Management System Documents Required for ISO/IEC 27001 Certification [Електронний ресурс] / O. Salah, G. Hinson. – Режим доступу: http://www.iso27001security.com/ISO27k_mandatory_ISMS_documents.rtf.

[6] SAS® Security Intelligence [Електронний ресурс]. – Режим доступа: https://www.sas.com/software/security-intelligence

[7] Security Intelligence Operations [Електронний ресурс]. – Режим доступу: http://tools.cisco.com/security/center/home.x

[8] М. В. Гайворонський, О. М. Новіков, Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009. – 608 с.

[9] Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою (ISO/IEC 27002:2005, MOD). ГСТУ СУІБ 2.0/ISO/IEC 27002:2010. –К.: Національний банк України, 2010. –163 с.

[10] Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2005, MOD). ГСТУ СУІБ 1.0/ISO/IEC 27001:2010. –К.: Національний банк України, 2010. –49 с.