Універсальний набір кіберзахисника

Компанія «Оберіг IT», як дистриб'ютор комплексних рішень у сфері кібербезпеки, знає, які інструменти зараз найбільш потрібні. Розповідає Олексій МУДРИЦЬКИЙ, менеджер з розвитку бізнесу «Оберіг IT».

Олексій МУДРИЦЬКИЙ,
менеджер з розвитку бізнесу компанії «Оберіг IT»

Зрілість підходів українських компаній до захисту власних активів та даних користувачів на сьогодні залишається дуже неоднорідною. Є достатньо просунуті організації з різних сфер діяльності, які вже використовують або розглядають використання у найближчому майбутньому найбільш передових рішень кіберзахисту. Є й інші (здебільшого державні), де рівень кіберзахисту досі на невисокому рівні. Відповідно більш захищеними є компанії, що мають такі рішення – починаючи від мережевих екранів, антивірусів, систем управління привілейованим доступом (PAM), DLP, SaaS-рішень для захисту інформації в хмарі на кшталт CASB, і закінчуючи власними SOC з командами аналітиків і офіцерів безпеки, які швидко реагують на інциденти. Але є й компанії, які в кращому разі використовують мережеві екрани та антивіруси.

Наразі ми бачимо великий попит на рішення, призначені для раннього виявлення ознак складної цілеспрямованої кібератаки й ефективної протидії загрозам «нульового дня». Так, стали затребуваними сервіси і системи (наприклад, Tenable Attack Surface Management), які надають командам безпеки максимальні можливості для спостереження за власними високотехнологічними активами – тобто ресурсами (у першу чергу веб-застосунками), доступними у глобальній мережі Інтернет, – і, зокрема, для візуалізації та постійного моніторингу «поверхні атаки». Через складність IT-інфраструктур і високу динаміку розвитку бізнесу далеко не всі такі ресурси вдається своєчасно навіть поставити на облік, не те що проконтролювати їхню захищеність. Тому такий «погляд ззовні» дуже важливий для розуміння того, як виглядає організація для потенційних зловмисників.

В цьому розрізі доцільно окремо згадати досить новий клас рішень, призначений саме для введення в оману зловмисників – системи класу Deception. Одним з найкращих прикладів на ринку України є Deception-система від американського виробника – компанії Fidelis Cybersecurity. За допомогою Deception-системи можна «збагатити» реальну IT-інфраструктуру мережею хибних цілей, які заплутуватимуть нападників, відводитимуть вектор атаки від реальних ресурсів, дозволятимуть швидко виявляти спроби реалізації загроз.

Також попитом користуються системи контролю і моніторингу дій привілейованих користувачів (наприклад, FUDO PAM і Delinea Secret Server) та засоби мультифакторної автентифікації. Масова віддалена робота зробила практично неможливим ізолювання критичних компонентів IT від глобальної мережі, а це призводить до стрімкого зростання безпекових ризиків. Адже якщо буде скомпрометовано обліковий запис звичайного користувача, реалізувати кібератаку все ще складно, а от наслідки викрадення облікових даних адміністратора можуть бути для організації катастрофічними. Тому побудова багатошарової системи безпеки на цьому напрямку є надзвичайно актуальною і, на нашу думку, залишиться в тренді.

Важливим завжди був і залишається захист від вірусів. Але вже минули ті часи, коли достатнім вважався «звичайний» антивірус, що працює за принципом порівняння підозрілих файлів і програм з базою сигнатур шкідливого коду. Сучасні інструменти кіберзловмисників уміють приховувати свій вміст, динамічно змінюватись. Це нерозв'язне завдання для «звичайного» антивірусного ПЗ. Тут на допомогу приходять системи нового покоління, які дозволяють постійно відстежувати, в першу чергу, поведінку файлів та процесів і ефективно блокувати шкідливі дії навіть умовно легітимного ПЗ. Мова про рішення класу Endpoint Detect & Response. І знову як приклад можна назвати компанію Fidelis Cybersecurity з її EDR-системою, котра до того ж інтегрується в єдиний комплекс з іншими рішеннями від цього виробника, в тому числі й зі згаданою вище Deception-системою.

Одним з ключових векторів атак є витоки конфіденційної інформації підприємств, тому для захисту підійдуть рішення Data Lost Prevention від Symantec або Forcepoint – лідерів ринку в царині захисту від витоків конфіденційної інформації. Дані рішення впроваджуються в інфраструктурі компанії і, послуговуючись налаштованими правилами і процесами, запобігають цілеспрямованому або помилковому переміщенню такої інформації за периметр організації.

Наостанок слід обов'язково згадати про захист технологічних мереж. Маємо на увазі мережі промислових та енергетичних компаній. Це досить специфічна галузь кібербезпеки, про неї складно розповісти двома словами. Потрібно лише знати, що ефективні інструменти захисту є і для них, зокрема від такого відомого виробника, як Tenable.

Щось прогнозувати, особливо у високодинамічній галузі IT/ІБ, – дуже невдячна робота. В найближчому майбутньому так само залишиться стандартний набір атак: фішинг, рейдерство, вимагання викупу, злам електронної пошти та соціальних мереж і т.д. Проте з'являється новий тип атак, спрямований на незахищені пристрої (датчики, побутова техніка, автомобілі, медичне обладнання тощо), які підключаються до Інтернету або об'єднуються в спеціалізовані мережі, це очікує і нас в Україні, коли закінчиться війна, оскільки даний тип загроз вже розглядається як сьогоденна реальність у країнах, які використовують мережі 5G.

Отже, точно можна сказати, що продовжуватиметься зсув у напрямку застосування перелічених класів рішень, а також важливими будуть питання забезпечення захисту Internet of Things і безпека технологічних мереж. Ну, і штучний інтелект... Куди ж без нього!

Щоб отримати більше інформації про передові рішення кіберзахисту, звертайтесь:
e-mail: info.ua@oberig–it.com
(044) 594 54 61