SANS

ість методів захисту, які змусять зловмисників плакати від безсилля

Кіберкриза між Росією й Україною

Ви маєте можливість здобути перемогу, захищаючи інформаційну безпеку. Ми продемонструємо вам, як це зробити.

У цьому документі наведено 6 неймовірно ефективних методів захисту. Вони будуть дієвими для організацій будь-яких розмірів.

Мета цих засобів реагування — не тільки припинення дій зловмисників. Натомість ми створюємо петлю позитивного зворотного зв'язку. Якщо ви будете дотримуватися наведених кроків, ви зменшите вплив наявних перешкод, що дозволить вам виконувати більш значущу роботу, а це, в свою чергу, ще більше зменшить вплив перешкод і так далі!

Якщо ви колись відчували, що виконуєте нескінченну, одноманітну та нудну роботу, пов'язану з IT або кібербезпекою, вам підходить цей план виправлення ситуації. Це план перемоги в ролі захисника.

Один ключовий елемент: вам НЕ слід відразу думати про придбання готових рішень у сфері інформаційної безпеки.

Процес закупівель у вашій організації, ймовірно, занадто тривалий.

Через поточні проблеми з ланцюгом поставок поставка таких програмно-апаратних засобів займає тижні (або більше).

Потрібен певний час для розгортання щойно придбаних комплексів і, у багатьох випадках, навіть додатковий час для інтеграції їх у вашу систему безпеки.

Через ці обмеження в сфері забезпечення новими інструментальними засобами ми зосередимося на тому, щоб максимально використати наявні інструментальні засоби. Коротше кажучи, ми плануємо застосовувати творчий підхід.

Ваш шлях до перемоги включає шість нижченаведених методів

1. **Виправлення**
2. **Виконання тактично правильних й ефективних стратегій журналювання подій**
3. **Керування вихідним трафіком (і геоблокуванням)**
4. **Планування й тестування швидких заходів захисту.**
5. **Впровадження системи керування застосунками**
6. **Досягнення стійкого «стабільного стану»**

Для кожного з перерахованих вище пунктів ми продемонструємо вам нижченаведене

- Для чого це потрібно
- Як це зробити (з упором на використання існуючих систем або недорогих рішень)
- Поширені помилки та як їх уникнути

Використання цього документа

Щоб забезпечити захист ваших даних, необхідно здійснювати ретельний і постійний контроль. У цьому документі ми продемонструємо ключові стратегії радикального зниження рівня зусиль, необхідних на тактичному рівні.

Методи, рекомендовані на цьому ресурсі, не розглядаються як радикальне відхилення від технологій, які використовуються в IT або системах інформаційної безпеки. Однак для деяких організацій ці викладені методи означають необхідність кардинальних змін. Автори цієї статті наполегливо рекомендують вам швидко розглянути всі шість нижченаведених кроків. Якщо ваша організація не виконує відповідні завдання, ви, ймовірно, набагато менше захищені від дій зловмисників, ніж ви уявляєте.

Ми наполегливо рекомендуємо розглядати елементи цього списку в тому порядку, в якому вони представлені. Вони наведені в порядку впливу. Однак, якщо один із пунктів занадто складний або проблематичний, пропустіть його. Краще пропустити кілька кроків і досягли певного рівня успіху, ніж зупинитися на будь-якому етапі.

На відміну від інших стратегій, викладені тут завдання мають бути частиною ітераційного процесу вдосконалення. Сподіваємося, що ви неодноразово будете переглядати цей план дій. Щоб полегшити такий перегляд в майбутньому, ми виділяємо можливі наступні кроки, які потрібно зробити після того, як ви повернетеся до цих завдань.

1 Виправлення

ДЛЯ ЧОГО ЦЕ ПОТРІБНО

Агентство з кібербезпеки та безпеки інфраструктури США (CISA) опублікувало інформацію щодо 383 уразливостей в Каталозі відомих використаних уразливостей. Ці вразливості регулярно використовуються кількома суб'єктами загроз для отримання початкового доступу, підвищення рівнів доступу або переміщення всередині мережі. Застосування відповідних виправлень до ваших систем ускладнить ці три дії. З урахуванням того, що загальна кількість становить 383 уразливості, 382 з *них можна усунути шляхом виправлення*! Залишилася одна? Вона стосується продукту, термін служби якого вже закінчився, тому виправлення недоступне.

ЯК ЦЕ ЗРОБИТИ

First, prioritize your patching efforts by ease of exploitation by a remote attacker. Broadly speaking, this means patch in the following order:

Система доступу до Інтернету та відповідне програмне забезпечення

- Мережа та засоби безпеки: брандмауери, концентратори VPN, балансувальники навантаження, проксі тощо
- Веб-сервери (Apache, Nginx, IIS тощо), веб-додатки, пристрої для роботи з електронною поштою, поштові сервери, FTP-сервери, SSH/SFTP
- Веб-застосунки
- Операційна система сервера віртуальних машин для систем доступу до Інтернету

Клієнти та програмне забезпечення клієнта

- ОС Microsoft Office
- Продукти Adobe PDF
- Браузери в порядку популярності (Chrome, Safari, Edge/Internet Explorer, Firefox)
- Клієнти VPN
- Мобільні пристрої та програмне забезпечення
- Оновлення ОС

Внутрішні сервери та серверне програмне забезпечення

- Сервери Windows
- Внутрішні веб-застосунки
- Пристрої Інтернету речей (IoT)

Використовуйте функції автоматичного оновлення програмного забезпечення та систем у вашому середовищі. Переконайтеся, що ці механізми оновлення налаштовані в операційній системі та ключових компонентах програмного забезпечення.

Оновлення ОС Microsoft:

- ОС Windows 10 і новіші версії ОС автоматично завантажують та встановлюють виправлення за допомогою служби Microsoft Update.
- Якщо ви розгорнули спеціальні параметри групової політики для Windows Update, переконайтеся, що в результаті цих налаштувань від користувачів не вимагається встановлення оновлень вручну. В інформації, доступної через нижченаведене посилання описується, як дозволити негайну інсталяцію автоматичного оновлення: Налаштування автоматичного оновлення за допомогою групової політики | Microsoft Docs

По-друге, проскануйте свою мережу на наявність відомих використаних уразливостей, опублікованих Агентством з кібербезпеки та безпеки інфраструктури США (CISA). Перевірка на наявність цих уразливостей здатна виявити системи, які залишилися неохопленими процедурою виправлення або є вразливими через неправильну конфігурацію.

Перевірка на наявність уразливостей

Якщо ваша установа відноситься до федеральних, державних, місцевих, племінних, територіальних урядів або організацій критичної інфраструктури державного та приватного секторів, CISA безкоштовно надасть вам послуги з кібер-гігієни, які включають перевірку уразливостей та веб-застосунків.

Якщо ви є клієнтом Qualys, перегляньте нижченаведену інформаційну панель, щоб зосередитися на відомих використаних уразливостях, опублікованих Агентством з кібербезпеки та безпеки інфраструктури США (CISA). Якщо ви є клієнтом Tenable.SC, можете також скористатися попередньо налаштованою інформаційною панеллю.

ПОРАДИ ЩОДО ТОГО, ЯК УНИКНУТИ ПОШИРЕНИХ ПОМИЛОК

Пастка «Я ПОВИНЕН все це виправити»

Іноді просто неможливо виправити систему. Або є ймовірність, що здійснення виправлення займе занадто багато часу. Враховуючи те, що ви перебуваєте в кризовому стані, це звучить дивно, але вам НЕ слід витрачати занадто багато часу на спробу примусового виправлення. Замість цього ізолюйте відповідну систему через мережу або брандмауери на основі вузлів, щоб обмежити доступ до решти вашої мережі. Багато програм безпеки зосереджуються на помилкових намірах: «ми повинні виправити все, перш ніж перейти до наступного елемента». Це майже ніколи не є гарною ідеєю. Вам слід виправити те, що ви здатні виправити, якщо це взагалі можливо, але якщо ви не можете щось виправити, *ізолюйте це і рухайтеся далі!*

Аналітичний параліч

Тестування виправлень може зайняти повний робочий день. Якщо ви застосовуєте виправлення від видавця програмного забезпечення, вам, швидше за все, можна просто розгорнути виправлення в невиробничій інсталяції або в менш критичній системі, щоб переконатися, що нічого не зламалося.

Якщо ви особливо стурбовані тим, що застосування виправлень може щось порушити, розгляньте можливість поетапного впровадження виправлень після короткого тестування, не пов'язаного з виробничим процесом. Багато організацій використовують поетапний підхід, коли виправлення здійснюються у незначній кількості систем (з використанням декількох систем тестування), деяких системах (10 %), багатьох системах (30 %) і, нарешті, у всіх системах, що залишилися. Забезпечте безпеку своїх найбільш чутливих систем до кінця впровадження виправлення. Якщо ви відчуваєте, що витрачаєте занадто багато часу та зусиль на виправлення, то, ймовірно, це так і є.

Впровадження виправлення також у разі проблем з низьким і середнім рівнем серйозності

Усвідомити вразливості досить важко. Іноді кілька вразливостей «низького» або «середнього» рівня серйозності можуть бути тісно пов'язані між собою й в результаті призвести до сукупного ризику, набагато вищого, ніж індивідуальний ризик кожної вразливості. Якщо рівень серйозності вразливості використовується для того, щоб виправляти *тільки* вразливості «найкритичнішого» рівня, це може поставити вас під загрозу сукупного ризику, значно вищого, ніж очікуваний.

Виправлення поза межами ОС

Переконайтеся, що ви одночасно впроваджуєте виправлення для некерованого клієнтського програмного забезпечення, як-от: сторонніх браузерів, продуктів Adobe тощо. Ці клієнти є типовою мішенню для зловмисників і часто не піддаються виправленню роками. Поточна модель для багатьох клієнтських програм — сповіщення користувачів про доступні оновлення, але не примусове їх встановлення. Не дозволяйте цим застосункам вислизати з поля зору системи захисту.

▶▶▶ МОЖЛИВИЙ НАСТУПНИЙ КРОК

Якщо перевірка виправлення займає занадто багато часу, подумайте про автоматизацію ключових елементів процесу. Прикладаючи менше зусиль в довгостроковій перспективі, можна створити бібліотеку модульних тестів. Ці тести є досить зручними з багатьох причин, але вони особливо ефективні для перевірки виправлень.

Apache JMeter — це безкоштовний інструмент, який дозволяє реєструвати практично будь-які дії на комп'ютері. Чому б не використати його для запису важливої бізнес-операції? Якщо ви маєте відповідний запис, ви можете радикально прискорити процес виправлення.

Після випуску наступного набору виправлень використовуйте нижченаведений робочий процес:

- У невиробничому середовищі переконайтеся, що записана транзакція продовжує виконуватися належним чином.
- Після цього скасуйте цю транзакцію.
- Застосуйте виправлення.
- Запустіть записану транзакцію.
- Переконайтеся, що транзакція відпрацювала належним чином.
- Якщо транзакція відпрацювала, перевірка виправлення виконана!

Активний пошук «втрачених» систем

Не припускайте, що ваші системи інвентаризації є точними. Займайтеся пошуком систем, які вислизнули з поля зору системи захисту і залишаються некерованими. Перевірка на наявність вразливостей може допомогти, але розглянемо також широкомасштабні системи перевірки Nmap, Masscan або подібні, призначені для виявлення некерованих вузлів.

Крім того, шукайте в своїх журналах ознаки неочікуваних вузлів. Ваші журнали DHCP, DNS і Active Directory є чудовими джерелами пасивного пошуку «втрачених» систем.

2 Виконання тактично правильних й ефективних стратегій журналювання подій

ДЛЯ ЧОГО ЦЕ ПОТРІБНО

Якщо у вас не впроваджено журналювання, у вас обмежена видимість. Журнали — це ваші очі і вуха, коли мова йде про все, що базується на застосуванні комп'ютерної техніки. Без журналів ви майже не матимете розуміння того, що відбувається у вашому середовищі. Крім того, за умови відповідного журналювання, процеси аудиторських перевірок та інших нормативних перевірок відбуватимуться швидше та легше.

ЯК ЦЕ ЗРОБИТИ

Якщо ви є організацією, яка використовує можливості хмарної електронної пошти та автоматизованої офісної системи, вам слід використовувати власну функцію журналювання, яке вже є в наявності. Зрештою, ви заплатили за ці функції за умови підписки. Якщо ваша організація використовує M365, вам слід почати з вбудованого Центру безпеки. Якщо ви використовуєте Google Workspaces, ви можете ознайомитися з журналюванням подій системи захисту в Центрі звітування для адміністратора.

Щодо організацій, які все ще працюють в локальній системі, вбудованим і потужним рішенням є механізм Windows Event Forwarding (WEF). Він дозволяє системам Windows здійснювати потокову передачу подій (журналів) у систему Windows Event Collector. Microsoft надає інструкції щодо використання механізму WEF для виявлення дій зловмисників у вашому середовищі.

ПОРАДИ ЩОДО ТОГО, ЯК УНИКНУТИ ПОШИРЕНИХ ПОМИЛОК

Не покладайтеся на параметри за замовчуванням

Іноді ми надто довіряємо нашим постачальникам. Швидше за все, вони не були членами вашого оточення. Вони не працювали безпосередньо з вами та вашою командою. Через це рівні журналювання за замовчуванням є для них найкращим припущенням і, ймовірно, не відображають ваших фактичних потреб щодо журналювання. Хто краще знає, що вам потрібно? Саме ви!

Замість того, щоб надто покладатися на постачальника, вам слід запитати себе: «Якими послідовностями подій я хочу поділитися?» Якщо ви хочете зловити зловмисників, які намагаються перебором даних для входу ввійти в систему, вам потрібно знати, коли відбувається помилка входу. Підхід, заснований на історії, зазвичай називається журналюванням на основі варіантів використання.

Журналювання — це постійний процес

У міру того, як ви будете просуватися на шляху до журналювання, ви дізнаєтеся про різні варіанти використання та журнали, які вам треба буде збирати та аналізувати. Це означає, що ваш підхід до журналювання з часом зміниться. Вам слід спланувати та сформувати очікування щодо того, що журналювання є ітеративним проектом. Організації, які успішно виконують журналювання, часто застосовують поетапний підхід.

Етап 1. Почніть з веб-сайту, призначеного для навчальний цілей, як-от what2log.com (який містить поради щодо того, що потрібно журналювати та як це робити).

Етап 2. Після цього застосуйте якісь більш рішучі дії. Щодо систем під керуванням ОС Windows, у Посібнику Microsoft із журналювання наведено дуже детальну інформацію.

Етап 3. Нарешті, ви можете використовувати таку систему, як Sigma. Перегляньте ряд правил, щоб ознайомитися зі сповіщенням, яке вас цікавить. Переглядаючи залежності, перераховані для відповідного запису, ви дізнаєтеся про джерела журналів, які вам потрібно буде збирати.

Уникайте накопичення журналів

Існує спокуса ввімкнення всіх параметрів журналювання, але ви швидко потопитеся в потоці журналів, які мають невелику цінність або взагалі її не мають. Мало того, що буде накопичуватися занадто багато інформації, щоб її обробляти, це може коштувати значну суму з точки зору зберігання журналів, використання мережі та будь-яких ліцензійних зборів, пов'язаних із вашими системами журналювання. Щоб подолати ці проблеми, ми закликаємо вас використовувати підхід, заснований на варіантах використання. Виберіть послідовність подій, якою ви бажаєте поділитися, а потім «поверніться назад». Які дані вам знадобляться, щоб поділитися цією послідовністю подій?

Обробляйте всі журнали таким чином, ніби вони є регульованими

Не всі журнали створені на рівних умовах... принаймні з точки зору вимог закону. У вас можуть застосовуватися нормативні або договірні вимоги щодо збереження журналів протягом певного часу (можливо, навіть років). Після ознайомлення з цими вимогами багато організацій повністю ухиляються від журналювання, оскільки вважають, що краще взагалі не журналювати й уникнути цих проблем зі збереженням.

На щастя, немає законів, які вимагають від організації зберігати *всі журнали* впродовж терміну зберігання інформації. Насправді, багато організацій, які мислять на перспективу, видаляють нерегульовані журнали, коли вони більше не потрібні. У деяких випадках можна без коливань видаляти журнал через тиждень.

▶▶▶ МОЖЛИВИЙ НАСТУПНИЙ КРОК

Для прискорення аналізу деякі організації вирішують збирати свої журнали в агрегаторах журналів або системі SIEM (система керування інформацією про безпеку та подіями інформаційної безпеки). Вибір, встановлення та розгортання такої системи — це велике починання, яке *не слід виконувати під час відповідного процесу пріоритизації та антикризового реагування*. Щоб краще зрозуміти важливість цієї роботи, радимо переглянути документ SANS для читального залу «Керівництво оцінювача системи нового покоління NextGen SIEM». Якщо у вашій організації вже встановлено систему типу SIEM, ознайомлення зі змістом цього керівництва все одно буде корисним. Можливо, ви використовуєте інструменти не в повній мірі.

Як потенційний проміжок перед тим, як отримати повноцінний інструмент SIEM, розгляньте можливість використання засобів для кореляції подій і полуавтоматизованих засобів аналізу, як-от WEFC, в якому використовується механізм WEF для сприяння централізації аналізу.

❸ Керування вихідним трафіком (і геоблокуванням)

ДЛЯ ЧОГО ЦЕ ПОТРІБНО

Контроль і моніторинг вихідних мережевих комунікацій є одним із найефективніших способів виявлення та порушення передачі експлойтів, інформаційного наповнення, а також командно-контрольного трафіку. Для більшості складових частин атак зловмисникам необхідно підключення до мережі, при цьому обмеження вихідного трафіку лише до абсолютно необхідного ускладнює процес атаки.

ЯК ЦЕ ЗРОБИТИ

Існує незліченна кількість способів досягти цього, але основними компонентами є правила брандмауера, фільтри веб-вмісту, фільтрація вмісту DNS та інструменти моніторингу мережі. Давайте розглянемо кожен із них.

Правила брандмауера

Ніколи не варто недооцінювати ефективність правил вихідного трафіку в брандмауері. Хоча вони є максимально ефективними, одночасно вони можуть бути складними в керуванні. Розумно створювати списки блокування на основі відомих шкідливих IP-адрес або навіть географічного розташування на основі діапазонів IP, зафіксованих в регіональних Інтернет-реєстрах. Інструмент RIRTools Джоффа Тайера робить це швидко і активно підтримується.

Фільтрування веб-вмісту

Більшість інтернет-сайтів класифікується різними компаніями, які фільтрують веб-вміст. Веб-канали цих продуктів дають чудову можливість фільтрації інтернет-трафіку на основі відомих категорій. Завдяки цьому можна надавати дозвіл на доступ до певних категорій або блокувати його, при цьому можна блокувати доступ до некласифікованих доменів. Менш складний командно-контрольний трафік здійснюється за допомогою нещодавно зареєстрованих доменів, які, ймовірно, ніколи не були класифіковані. Отже, блокування некласифікованих доменів ускладнює завдання. Фільтрація веб-вмісту зазвичай виконується на брандмауерах нового покоління або через веб-проксі. Якщо у вас немає засобу забезпечення безпеки з цим набором функцій, гідною альтернативою є фільтрація вмісту DNS.

Фільтрація вмісту DNS

Той самий підхід до «категоризації», який використовується фільтрами веб-вмісту, застосовується в деяких DNS-серверах. Це дозволяє DNS-серверу повертати фактичну IP-адресу веб-сайту, якщо категорія дозволена, або IP-адресу веб-сторінки, яка вказує, що домен був заблокований службою фільтрації. Недоліком цього підходу є припущення, що для систем, залучених до атаки, зловмисник використовує DNS-імена доменів. Якщо зловмисник використовує прості IP-адреси, ця фільтрація буде неефективною. Також вимагається, щоб усі системи в середовищі використовували відповідні DNS-сервери. Тому дуже важливо так налаштувати правила брандмауера для вихідного підключення, щоб дозволити направляти трафік DNS лише службі фільтрації вмісту DNS. Якщо можливо, краще дозволити лише довіреним внутрішнім DNS-серверам зв'язуватися із зовнішніми системами DNS, а також забезпечити, щоб всі вузли внутрішньої мережі використовували внутрішні DNS-сервери вашої організації.

Крім того, розгляньте можливість впровадження утиліт freq.py, freq_server і domain_stats.py Марка Баггетта. Ці інструменти допомагають ідентифікувати шкідливі домени, або згенеровані алгоритмічно або створені нещодавно. Автор докладно пояснив використання інструментів на конференції Security Onion; обов'язково ознайомтеся з останньою версією інструментів, які там згадувалися.

Інструменти моніторингу мережі

Мета цього документу — надати інструменти та архітектури, які можна швидко розгорнути, якщо вони ще не встановлені. Хоча серйозна вихідна фільтрація на основі «списків довірених», яка застосовується до конкретних веб-сайтів, служб та IP-адрес, гарантує, що система не обмінюється даними з ненадійними вузлами в Інтернеті, це висока мета, яка може бути недосяжною. Коли ви працюєте над досягненням такої високої мети, дуже важливо мати ефективну систему моніторингу мережі, щоб покращити видимість, необхідну для виявлення зловмисника, який обішов інші методи фільтрації, які ми обговорювали.

ПОРАДИ ЩОДО ТОГО, ЯК УНИКНУТИ ПОШИРЕНИХ ПОМИЛОК

Розглянемо відкритий код

У більшості сфер IT та безпеки існує поєднання рішень з відкритим кодом і комерційних рішень. У сфері моніторингу та аналізу мережі рішення з відкритим кодом зазвичай мають більше функцій, ніж аналогічні комерційні пропозиції. Якщо використання рішень з відкритим кодом є проблематичним, оскільки вашій організації потрібна професійна підтримка, розробники цих програм зазвичай пропонують професійне обслуговування або співпрацюють з компетентними постачальниками (й пропонують їхні послуги).

Скористайтеся модульним підходом

Як уже згадувалося в цьому розділі, покращення видимості та контролю на мережевому рівні може вважатися серйозною справою. Більшість проектів керування мережею зазнають невдачі через занадто велику область застосування. Набагато простіше розгорнути цілеспрямований набір елементів керування в групі настільних ПК, які використовуються користувачами з високим ризиком або, можливо, стратегічно важливих серверів.

▶▶▶ МОЖЛИВИЙ НАСТУПНИЙ КРОК

Розгляньте можливість сегментації вашої мережі на функціональні зони, щоб обмежити здатність зловмисників отримувати доступ до ресурсів після отримання доступу до одної системи. Якщо ваша мережа вже сегментована, подумайте про перехід до мережі з топологією мікросегментації.

4 Планування й тестування швидких заходів захисту

ДЛЯ ЧОГО ЦЕ ПОТРІБНО

Одна річ, яку багато захисників неправильно розуміють, — це швидкість атаки. Слід почати планування способів, здатних розладнати плани ваших супротивників у режимі реального часу. Такі дії, як відключення систем або навіть сегментів мережі під час атаки, завадять зловмисникам досягти своїх цілей.

ЯК ЦЕ ЗРОБИТИ

Ізолюйте системи або мережі

У процесі співробітництва з власниками системи визначте, які системи можна перевести в автономний режим, і за яких умов. Ми настійно рекомендуємо вам скористатися цією формою (попередня авторизація, щоб перевести систему або мережеву зону в автономний режим). (Див Додаток А ▶)

Якщо у вас є підстави вважати, що система скомпрометована, вам потрібно діяти швидко. Як правило, найкраще від'єднати її від мережі. Це дозволяє зберегти та зібрати найбільшу кількість доказів. Радимо ДО виникнення інциденту звернутися до свого постачальника послуг з реагування на інцидент, щоб визначити, які докази їм знадобляться. Ви повинні конкретно запитати, чи планують вони робити аналіз пам'яті. Якщо вони збираються це робити, дуже важливо запобігти вимиканню системи до моменту, поки вони явно не попросять вас це зробити. Вимкнення системи очищає цю пам'ять, позбавляючи їх ключових доказів, які вони збираються використовувати.

Заблокуйте облікові записи або можливість скидання паролів

Зловмисники часто використовують для своїх цілей дійсні облікові записи користувачів. Будьте готові швидко заблокувати облікові записи або можливість скидання паролів для кількох порушених облікових записів. Будьте готові видалити облікові записи з груп, до яких вони не належать.

ПОРАДИ ЩОДО ТОГО, ЯК УНИКНУТИ ПОШИРЕНИХ ПОМИЛОК

Практичні рекомендації

Багато організацій недооцінюють рівень зусиль, необхідних для скоординованого виконання цих дій. Перш ніж спробувати виконати технічне тестування, спершу проведіть «теоретичні» заходи, щоб переконатися, що різні групи, які необхідні для координації цієї діяльності, розуміють, яку роль вони відіграють у процесі.

Прогнозування наслідків у порівнянні з вдосконаленням процесу

▶▶▶ МОЖЛИВИЙ НАСТУПНИЙ КРОК

Створіть сценарії (за допомогою PowerShell або скористайтеся якимись інструментами автоматизації), щоб виконувати ці дії швидким і послідовним способом.

Важливо перевіряти ефективність роботи, щоб переконатися, що виконана робота відповідає очікуванням. Необґрунтовано та контрпродуктивно застосовувати знання щодо дій, які були зроблені сумлінно під гарячу руку, після того, як все завершилося. Припустимо, що дії, які вживали люди, були засновані на найкращій доступній інформації, яку вони мали на той час. Спробуйте зосередитися на тому, як швидше надати точнішу інформацію, щоб усі були краще поінформовані під час наступної події реагування на інцидент.

5 Впровадження системи керування застосунками

ОСОБЛИВА ПРИМІТКА

Для більшості організацій цей розділ, ймовірно, буде найскладнішим у застосуванні. Незважаючи на труднощі, він залишиться в цьому списку, оскільки він є надзвичайно ефективним для припинення багатьох атак.

ДЛЯ ЧОГО ЦЕ ПОТРІБНО

Керування застосунками (раніше це називалося: «ведення списків дозволених застосунків») — це технологія, яка дозволяє обмежувати роботу програм, які можна запускати на комп'ютері. Це запобігає запуску зловмисниками шкідливих програм, які вони розміщують у вашій системі.

Важлива примітка. Вправні зловмисники знають, як обійти систему керування застосунками, як будь-які засоби контролю безпеки. Однак це непросто. Не кожен зловмисник зможе це обійти. Найчастіше при цьому вони створюють багато перешкод. Увімкнувши систему керування застосунками, ви можете почати шукати ознаки незвичної поведінки. Одним з найкращих засобів виявлення є наявність попередження про те, що користувачі шукають запущені інструменти керування застосунками.

ЯК ЦЕ ЗРОБИТИ

Якщо у вас є інструмент стороннього розробника, який здатен керувати застосунками, спробуйте використовувати його. Якщо такий інструмент відсутній, ОС Windows має вбудований інструмент керування застосунками під назвою AppLocker. Усі версії ОС Windows 10 і 11 зараз підтримують цю потужну функцію. Продукти Microsoft оснащені посібником із застосування функції AppLocker. Уважно дотримуйтеся наданих інструкцій, розгортаючи функцію в невиробничому середовищі, перш ніж розгортати її у виробничих системах.

ПОРАДИ ЩОДО ТОГО, ЯК УНИКНУТИ ПОШИРЕНИХ ПОМИЛОК

Профіль щодо фактичного використання

Якими б потужними не були ці інструменти, якщо ви допустите помилку в конфігурації (заблокуєте необхідний застосунок), це може перешкодити системі працювати так, як потрібно користувачеві. Найшвидший і найбезпечніший спосіб створити конфігурацію — це заснувати її на фактичній поведінці користувача.

Якщо у вас є програма, яка відстежує поведінку користувачів, скористайтеся нею. Деякі стандартні інструменти сторонніх розробників, які роблять це, — агенти виявлення й реагування кінцевих точок (EDR), агенти керованого виявлення й реагування (MDR), а також форензики.

Якщо у вас немає жодного з цих продуктів, інший варіант — скористатися перевагами маловідомої функції Windows. Усі використовувані програми відстежуються за допомогою моніторингу використання системних ресурсів Windows (SRUM). Він містить постійний 30-денний список програм, які запускалися всіма користувачами та системою. Використовуючи спеціалізовані інструменти, ви можете ознайомитися з базою даних SRUM. Мабуть, найпростіший інструмент для читання інформації з бази даних — програма SRUM-Dump.

Не поспішайте із примусовим застосуванням

Після створення політики керування застосунками правильним рішенням може бути запуск системи в режимі «аудит» або «навчання» протягом тижня або більш тривалого періоду. У цьому режимі роботи ви дізнаєтеся про застосунки, які були б заблоковані.

6 Досягнення стійкого «стабільного стану»

ДЛЯ ЧОГО ЦЕ ПОТРІБНО

Ми збираємося продемонструвати вам, як використовувати вищенаведені методи для створення стабільного стану, який дозволить вам закріпити успіх.

ЯК ЦЕ ЗРОБИТИ

Запровадження надійного контролю безпеки — це марафон, а не спринт. Не поспішайте. Багато організацій намагатимуться раптово «серйозно зайнятися безпекою» і спробувати все виправити відразу. Це не тільки заважає вирішенню поточних проблем, але й рідко спрацьовує як слід. Як і в результаті застосування будь-якої персональної програми фізичної підготовки, ви, як правило, отримуєте кращі результати, вносячи невеликі впливові зміни, які призводять до поступового прогресу з часом.

ПОРАДИ ЩОДО ТОГО, ЯК УНИКНУТИ ПОШИРЕНИХ ПОМИЛОК

Усунення перешкод дає змогу зосередитися

Ми спеціально зосередилися на захисних і розпізнавальних засобах керування, які, крім ефективності, УСУВАЮТЬ ПЕРЕШКОДИ з вашого середовища. Це, в свою чергу, дозволить вам більше зосередитися на важливих речах (зокрема, усунути ще більше перешкод!).

Бережіть свій час для вдосконалення процесу

Досить скоро ви створите петлю позитивного зворотного зв'язку, де щоразу після вдосконалення видимості й елементів керування ви отримуватимете більше часу, щоб покращувати речі. Якщо ви потрапляєте в ситуацію, в якій відчуваєте, що «все горить», методи, які ми розглянули в цьому документі, призначені для ВАС. Це може здатися дивним, але 2-годинна «пробка» на дорозі, де ви можете зосередитися та внести відчутні покращення в один із цих елементів керування, насправді окупиться багаторазово.

▶▶▶ МОЖЛИВИЙ НАСТУПНИЙ КРОК

Цей документ є ресурсом, який дає змогу перейти до ефективної програми безпеки. Радимо переглянути цей список кілька разів, щоб приділити увагу елементам, які вам довелося пропустити з метою економії часу. Після того, як вам стане зрозумілим цей список, перейдіть до глибшої та складнішої структури, рекомендованої Центром стратегічно важливих засобів забезпечення безпеки в Інтернеті.

Про авторів

Мік Дуглас, головний інструктор інституту SANS

Джон Горенфло, сертифікований інструктор інституту SANS

Додаток A

ПОПЕРЕДНЯ АВТОРИЗАЦІЯ ДЛЯ ВИВЕДЕННЯ СИСТЕМИ АБО МЕРЕЖЕВОЇ ЗОНИ В АВТОНОМНИЙ РЕЖИМ

Авторизація в системі

Щоб запобігти атаці на всю організацію, робочій групі [TEAM NAME] дозволяється перейти в автономний режим роботи в системі [SYSTEM NAME], якщо її члени вважають, що створюється загроза решті організації.

[Date]
[System owner, title]
[Response team person, title]

Авторизація в мережі

Щоб запобігти атаці на всю організацію, робочій групі [TEAM NAME] дозволяється перейти в автономний режим роботи в системі [NETWORK ZONE NAME], якщо її члени вважають, що створюється загроза решті організації.

[IMPACTED system owners, title]
[Response team person, title]

ПРИЧИНА ПЕРЕХОДУ В АВТОНОМНИЙ РЕЖИМ РОБОТИ В СИСТЕМІ АБО МЕРЕЖІ

Я, [Response team person, title] перейшов в автономний режим роботи в системі/мережі [system/network name] [DATE AND TIME], тому що вважав, що утворилася загроза для решти мережі. При цьому я сповістив власника системи [system owner].

Моє рішення ґрунтується на нижченаведеній інформації.

[Justification here]

Як елемент вдосконалення процесу, я розгляну це питання разом із [System owner, any other people] at [Future date, not more than 1 week out].

[Response team person, title][DATE]