CUA-15-04R
Рекомендації CERT-UA з протидії загрозі інсайдера

Автор: Іван Соколов
Державна служба спеціального зв'язку та захисту інформації України
Державний центр кіберзахисту та протидії кіберзагрозам
04119, Україна, м. Київ, вул. Мельникова, 83б
тел.: +380 44 281 88 25
факс: +380 44 489 31 33
www: cert.gov.ua

ЗМІСТ

1. Загальна інформація

Інсайдер — особа, що має доступ до інформації організації та навмисно або ненавмисно порушує вимоги щодо конфіденційності цієї інформації.

Для того, щоб було зрозуміла загроза, про яку йдеться у цій публікації, наведемо кілька прикладів інсайдерських загроз (insider threats).

Приклади:

1. Система моніторингу безпеки організації зафіксувала глибокої ночі з'єднання ззовні до мережі організації та спробу зараження шкідливим програмним забезпеченням.

2. Програміст, змінюючи роботу в організації, краде вихідні коди програмного продукту, який належить організації.

3. Група співробітників організації, співпрацюючи з іншою організацією, переслідує корисливі інтереси та реалізує шахрайську схему.

4. Системний адміністратор організації, який довго працював, звільняється, оскільки не задоволений заробітною платнею, запропонованою новим керівництвом.

Багато керівників, співробітників та звичайних людей не розуміють величини загрози, яку потенційно несуть інсайдери. Фактично, з цим видом небезпеки для організації стикаються дуже часто, причому більшість невеликих організацій не мають уявлення щодо плану дій для протидії. Часто організації стикаються з типовими для їхнього типу діяльності інсайдерами, причому ці випадки зазвичай мають періодичний характер.

Команда CERT-UA під час своєї діяльності стикалась з випадками, коли одна людина, яка була системним адміністратором, фактично могла шантажувати керівників, вивести з ладу комп'ютерні мережі і системи, суттєво та у гіршу сторону впливати на розвиток усієї організації і, навіть, повністю ігнорувати діючі політики та процедури організації.

Виконайте 10 простих порад CERT-UA для того, щоб мінімізувати потенційну шкоду від інсайдерської загрози та/або попередити її виникнення взагалі:

2. Рекомендації

1. Враховуйте досвід попередніх інцидентів

Для типових організацій інсайдерські загрози майже однакові і про способи протидії інсайдерам можна знайти багато, наприклад, у рекомендаціях на цю тему. Якщо Вас атакували, впровадьте відповідні засоби захисту. Деякі організації створюють команди з вивчення та протидії інсайдерським загрозам (Security Operations Center), розбору випадків і методик протидії їм.

2. Сконцентруйтесь на захисті критично важливих ресурсів

Більше третини інцидентів, пов'язаних з інсайдерами, за даними команд швидкого реагування, мають відношення до іноземних державних організацій. Проведіть аудит критично важливих цінностей організації, впровадьте надлишкові та посилені заходи та засоби для їх захисту. Уявіть, що Ваша організація втратила ці цінності, сплануйте дії на такий випадок. Уникайте "розлагодження" системи захисту організації. Ці завдання можуть бути споріднені з аудитом ризиків організації.

3. Використовуйте різноманітні способи захисту

Ефективніший багаторівневий та різнотипний захист, він значно ускладнить побудову вектору атаки на організацію. Вивчіть, що означають наступні ключові слова, якщо Ви опікуєтесь захистом від інсайдерів — DLP, SIEM, IDS, log management and analisys тощо. Ведіть та аналізуйте журнальні файли пристроїв захисту організації на предмет виявлення підозрілої активності.

4. Реагуйте на загрози від партнерів

Довірені бізнес-партнери (Trusted Business Partner, TBP), якими можуть бути контрактори або аутсорсингові компанії, можуть нести інсайдерську загрозу, не меншу за конкурентів. Визначте заходи з інформаційної безпеки у контракті з TBP. Вимагайте від TBP таких же заходів з захисту від інсайдерських загроз, які використовує Ваша організація. Захист бізнес-групи від інсайдера рівний захисту найменш захищеної компанії цієї групи. Робіть аналізи ризиків, політики безпеки та процедур (бізнес-процесів) TBP. Впроваджуйте для контракторів таку ж політику, як для співробітників Вашої організації.

5. Зважайте на взаємовідносини, як на індикатор інсайдерської загрози

Напружені взаємовідносини між організаціями — 4 місце серед причин інсайдерських випадків згідно CERT Insider Threat Database (зараз там близько 700 видів загроз). Погані відносини між співробітниками організації — 8 місце. Коли негаразди у колективі — найчастіше це стає причиною IT-саботажу через інсайдерів. Покращуйте атмосферу у колективі (make team gathering). Це не тільки збереже організацію, а ще й весело! :)

Деякі організації, також, навчають персонал, як виявляти типові індикатори інсайдера,

впроваджують HR-менеджмент та вводять посади відповідальних за внутрішню безпеку.

6. Навчайте персонал згідно потенційної посади

Працевлаштування — 3 місце у CERT Insider Threat Database. Обережно з'ясуйте, чи є у Вашій організації дані, системи чи інші ресурси, заради отримання яких Ваш персонал може бути підкуплений конкурентами. Робіть періодичні негласні перевірки співробітників на предмет того, чи заангажовані вони сторонніми організаціями.

7. Приділяйте особливу увагу перепризначенням та звільненням

Кадрові зміни — перше місце у CERT Insider Threat Database, тому необхідно робити цільовий моніторинг співробітників, які звільняються та змінюють посади у організації. Впровадьте особливі вимоги до персоналу у відношенні критичних для організації активів. Звільняючи обуреного співробітника IT-персоналу, робіть це швидко та рішучо (так, щоб він не мав технічної можливості нашкодити організації, в тому числі і віддалено), попередньо зробивши резервні копії критично важливих активів.

8. Формалізуйте та узгодьте з керівництвом питання приватності у організації

Приватність співробітників — важлива та щоб вона не стала інструментом інсайдера, треба приділяти їй увагу. Для цього треба узгодити питання приватності з керівником, в залежності від сектору (державний або приватний) та важливості (критична інфраструктура). Законодавство та правила можуть відрізнятись у різних країнах і сферах діяльності, а права людини порушуватись не повинні. Проте, треба знайти гармонійне поєднання корпоративної політики безпеки та приватності співробітників (часто це - робота юристів, HR та керівництва).

9. Працюйте з організацією комплексно

IT-персонал не може вирішити проблему інсайдерів власними зусиллями. Потрібні зусилля менеджменту, IT-персоналу, співробітників з інформаційної безпеки, власників даних, розробників програмних продуктів, керівництва та співробітників.

Іноді, для того щоб виявити інсайдера, треба провести велику роботу всередині підрозділу організації та налагодити ефективні відносини між підрозділами.

10. Створіть програму протидії інсайдерській загрозі

У перші три місяці треба:

- створити та заповнити вакансію топ-менеджера, що займеться інсайдерською проблематикою;

- сформувати команду з протидії інсайдерським загрозам;

- створити та погодити з керівництвом політику безпеки, яка включатиме інсайдерську загрозу;

- розробити процеси та впровадити засоби протидії інсайдерам.

У перші шість місяців треба:

- повністю переробити та значно покращити політику безпеки;

- регулярно перевіряти контрольні параметри для виявлення інсайдерів;

- налагодити заняття з персоналом стосовно інсайдерських загроз, моделюючи типові інсайдерські загрози у вигляді практичних занять;

- витрачати зусилля на team gathering, бо це весело!

2.1 Порядок рекомендованих CERT-UA заходів, пов'язаних із зміною особи, відповідальної за захист інформації та супроводження інформаційно-телекомунікаційних систем.

Назва етапу	Зміст робіт	Примітка
Отримання від адміністратора усієї інформації щодо систем та мереж	Адміністратор, що змінюється, повинен передати новопризначеному адміністратору та керівництву: - атрибути доступу до систем та мережевого обладнання; - інструкції з встановлення та обслуговування серверів та програмних складових (регламентного та екстреного обслуговування); - схеми мережі та систем, що діють; - носії даних, ПЕОМ, ключі від комутаційних шаф, серверних, перепустки, інші атрибути доступу до службових приміщень тощо. Звільнення адміністратора зі збереженням добрих стосунків — завжди кращий варіант для організації. Керівництво може запропонувати адміністратору премію у разі нормальної передачі справ та посади.	

	У більшості випадків доцільно одразу ж відсторонити адміністратора від доступу до активного мережевого та серверного обладнання, а також супроводжувати його при знаходженні у організації.	
Оптимізація розподілу повноважень	Необхідно вирішити, хто та за що буде відповідати після звільнення адміністратора. Якщо організація не велика, то територіальний принцип, за яким нові адміністратори відповідають за усе обладнання основної організації та її філіалів, буде кращим. Якщо сервіси та системи організації є складними, то кращим буде функціональний поділ повноважень, коли за певні сервіси організації відповідатимуть окремі спеціалісти.	
Зміна усіх поролів	На граничному активному мережевому та серверному обладнанні необхідно змінити адміністративні атрибути доступу до усіх сервісів. У першу чергу: - сервіси SSH та інші протоколи віддаленого управління, також треба переглянути налаштування щодо дозволених IP-адрес та ключів автентифікації, які приймають сервери SSH, перервати усі активні сесії; - адміністраторів веб-серверу та привілейованих користувачів сайтів; - пароль адміністратора домену та субдоменів; - пароль адміністратора поштового сервісу; - паролі від серверу контролю доступу (ACS) та на основному (в першу чергу — граничному для організації) активному мережевому обладнанні. Найчастіше це — маршрутизатор (router) та міжмережевий екран (pix firewall, проксі-сервер або шлюз мережі на базі Unix). Це найкращий час для впровадження більш жорсткої парольної політики, аудиту та видалення застарілих	

	облікових записів (адміністратор може користуватись обліковими даними, наприклад, звільнених співробітників), складання білінгового плану, оновлення паролів співробітників тощо. Якщо повний перелік обладнання для зміни паролів визначити не можливо, потребуватиметься незалежний аудит з наступною зміною паролів нововиявленого обладнання, яке не підконтрольне.	
Перевірка локальної мережі на віруси	Активне серверне обладнання та робочі станції усіх користувачів повинні бути перевірені на предмет встановлення шкідливого програмного забезпечення.	
Перевірка на виконання нештатних функцій	Активне мережеве та серверне обладнання повинно бути перевірене на предмет виконання не передбачених політикою безпеки та планом захисту завдань (шлюзи мережі в обхід основних пристроїв захисту, паразитні з'єднання у локальній мережі, несанкціоновані точки бездротового Інтернету, релеї електронної пошти, анонімні проксі-сервери тощо). Усі сервіси, що надаються активним мережевим та серверним обладнанням організації, повинні бути перевірені на необхідність і достатність.	
Оптимізація зовнішніх підключень	Усі підключення до зовнішніх для організації мереж повинні бути проаналізовані, бажано скласти логічну та фізичну схеми. На основі діючих договорів з провайдерами необхідно зробити висновок про оптимальність поєднання організації з Інтернетом та всередині організації. Часто необхідна оптимізація таких підключень, централізація питань моніторингу зовнішніх підключень до організації та моніторингу подій безпеки.	
Збір та узагальнення	Від адміністратора та користувачів треба отримати максимальну інформацію щодо проблемних питань,	

усіх проблемних питань щодо адміністрування та безпеки	нагальних завдань та перспектив напрямку адміністрування систем та мереж, а також щодо їхньої безпеки. Для цього доцільно провести зібрання усіх інших співробітників цього напрямку, наприклад, тих, що адмініструють філіали організації.	
Унеможливлення несанкціонованого фізичного доступу до організації	Адміністратору повинно бути заборонено: - наказом керівництва виконувати завдання з супроводження обладнання та його захисту; - організаційно-технічними мірами, наприклад, охоронною сигналізацією та службою безпеки повинно бути унеможливлене фізичне потрапляння адміністратора на об'єкти, що стосуються телекомунікаційних складових. Важливо розуміти, що навіть доступ його до одного порту одного комутатора на деякому поверсі може надати адміністратору можливість адмініструвати та нашкодити роботі активного мережевого та серверного обладнання. - доцільно запровадити (оновити за наявністю) контроль фізичних портів активного комутаційного обладнання по MAC-адресам (mac address policy, технологія 802.1x тощо).	

Зміни до документу

- 28.07.2015: Перший випуск.