DOI 10.37882/2223–2966.2023.04.32

МЕТОДЫ СНИЖЕНИЯ ВОЗМОЖНОСТЕЙ НАРУШИТЕЛЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ВЗГЛЯД НА ИНСАЙДЕРСКУЮ УГРОЗУ

METHODS FOR REDUCING AUTHORITY IN THE FIELD OF INFORMATION SECURITY: A LOOK AT THE INSIDER THREAT

V. Strizhkov

Summary. The article presents an assessment of existing insider mitigation methods used to mitigate the effects of insider attacks. Although both motive and opportunity are necessary to commit a crime, this article focuses on the concept of opportunity. Opportunity is more tangible than motive, hence it is more pragmatic to think about measures to reduce opportunities. For this purpose, theories of possibilities from the field of criminology are considered. The assessment offers several areas of study and can help organizations implement information security controls that reduce the opportunity for insiders. The evaluation is not final, but serves to inform future understanding.

Keywords: information security, insider, internal intruder, reduction of authority, insider threat reduction.

Стрижков Владислав Александрович
Аспирант, Федеральное государственное образовательное бюджетное учреждение высшего образования «Финансовый университет при Правительстве Российской Федерации» (г. Москва)
218668@edu.fa.ru

Аннотация. В статье представлена оценка существующих методов снижения возможностей внутреннего нарушителя, используемых для смягчения последствий инсайдерских атак. Хотя для совершения злодеяния необходимы как мотив, так и возможность, в данной статье основное внимание уделяется понятие возможности. Возможность более осязаема, чем мотив, следовательно, более прагматично размышлять о мерах по сокращению возможностей. С этой целью рассматриваются теории возможностей из области криминологии. Оценка предлагает несколько областей исследований и может помочь организациям в реализации средств управления информационной безопасностью, уменьшающих возможности внутренних нарушителей. Оценка не является окончательной, но служит для информирования будущего понимания.

Ключевые слова: информационная безопасность, инсайдер, внутренний нарушитель, снижение полномочий, сокращение инсайдерской угрозы.

Введение

По данным опроса CyberSecurity Watch [1], 46% респондентов считают, что вред, причиненный внутренними атаками, наносит больший ущерб, чем вред, причиненный внешними атаками. Исследование Boardroom Cyber Watch 2013 [2] фактически предупредило, что эта цифра может быть выше 50%. Инсайдер — это любое лицо, имеющее законный доступ к инфраструктуре информационных технологий (ИТ) организации. Хотя для совершения злодеяния необходимы как мотив, так и возможность, в этой статье основное внимание уделяется концепции возможности. Согласно Уиллисону [3], исследователям полезно размышлять о киберпреступлениях с точки зрения криминологических теорий, поскольку они, в конце концов, являются преступлениями. В криминологии четыре теории преступности воплощают перспективу теории возможностей: теория рационального выбора, теория рутинной деятельности, модель преступления и, совсем недавняя, теория ситуационного предотвращения преступлений (SCP) [11]. Поскольку теория SCP наиболее непосредственно развилась из вышеупомянутых теорий, она использовалась в качестве теоретической основы в исследовании. Существенное различие между внешними злоумышленниками и инсайдерами заключается в том, что те, кто действует извне, имеют ограниченные возможности для осуществления своей атаки. Они должны использовать уязвимости в системе, в то время как инсайдеры имеют привилегированный доступ и, следовательно, больше возможностей, однако инсайдер, в отличие от внешнего нарушителя, подчиняется политикам, процедурам и соглашениям.

Падаячи [14] приходит к выводу, что возможности для совершения преступления с точки зрения внутренней угрозы возникают из-за следующих трёх наборов обстоятельств: во-первых, инсайдеры способны определить возможности для совершения преступления в своей повседневной деятельности. Во-вторых, активы данных, которые являются ценными, видимыми, доступными и передаваемыми, открывают заманчивые возможности для киберпреступности. В-третьих, новые инновации и изменения постоянно создают новые

возможности для внутренних угроз. Когда Теохариду и др. [5] изучили ISO 17799 и его связь с решением проблемы внутренних угроз, они обнаружили, что теории преступлений, такие как теория SCP, не рассматривались в этом стандарте ISO, поскольку они не учитывали потенциальную сторону преступления. Это упущение в предыдущем и текущем стандарте указывает на то, что возможности нарушителей требуют дальнейшего изучения.

Теоретическая основа

В текущем систематическом анализе, т.е. обзоре, который включает критическую оценку и сопоставление информации систематическим и подотчетным образом, различные методы защиты информации сопоставляются с теорией SCP для составления каталога методов. Теория SCP рассматривает пять категорий мер по уменьшению возможностей, а именно: «увеличение усилий», «увеличение рисков», «уменьшение вознаграждения», «уменьшение провокаций» и «устранение оправданий». Каждая мера далее делится на 5 конкретных методов (то есть всего 25 подкатегорий) [12].

Увеличение усилий

Категория, вынуждающая «усилить усилие», включает в себя подтверждение восприятия того, что конкретное преступление будет трудно исполнить. Подкатегории, которые обсуждаются более подробно ниже: целевое упрочнение; контроль доступа на объекты; контроль вывода экрана; уклонение от правонарушителей и инструменты контроля (т.е. инструменты, которые могут быть использованы для причинения вреда).

Средства управления информационной безопасностью, предлагаемые для «защиты цели» (т.е. повышения сложности совершения преступления), включают антивирусное программное обеспечение [3]; исправление уязвимостей; изоляция чувствительной системы; правильная политика паролей; выборочная установка; закрытие посторонних портов и внесение в белый список. Антивирусы подвержены неправомерному использованию, а внесение в белый список легче осуществить, так как оно основано на ведении списка разрешенного программного обеспечения [7].

Брандмауэры неэффективны для внутренних угроз, поскольку работают в пределах своего периметра. Data Loss Prevention (DLP) контролирует исходящие данные и может быть более подходящим для защиты периметров, чем брандмауэры. Хиндуджа и Коой [8] также предлагают фильтрацию входа/выхода и ограничения на основе интернет-протокола (IP), которые существенно помогают контролировать трафик, входящий и исходящий из сети. Средства управления информационной безопасностью, предлагаемые для отвлечения нарушителей, включают приманки; расщепление ключей; разделение обязанностей и проверка биографических данных сотрудников (т.е. предварительная проверка) [3] и внешнее хранение данных [8]. Хотя приманки эффективны для сдерживания инсайдеров, могут потребоваться соглашения для покрытия вопросов ответственности. Разделение обязанностей предотвращает неправильное использование. Таким образом, как разделение ключей, так и разделение обязанностей являются средствами предотвращения сговора. Хотя методы предварительной проверки, такие как профилирование, не являются точными предикторами будущей угрозы, руководящие принципы ISO/IEC 27002 по безопасности человеческих ресурсов [9] предлагают многочисленные средства контроля, которые включают проверку биографических данных перед приемом на работу. Эти средства контроля способствуют тому, чтобы сотрудник придерживался политики безопасности организации во время работы и что права доступа удаляются при увольнении [9].

Контроль веб-доступа [10], фильтрация загрузок незаконных инструментов (т.е. контроль загрузок [3]); процедуры прекращения [3]; наименьшая привилегия; разрешение на доступ к файлам [8] и периодические проверки [8] были предложены в качестве мер информационной безопасности в отношении инструментов управления. Фильтрация загрузок является важным средством контроля, поскольку инсайдеры могут загружать незаконные инструменты, такие как регистраторы нажатий клавиш, чтобы помочь им в совершении злонамеренных действий. Принцип наименьших привилегий — еще один фундаментальный метод контроля; однако его практическое применение может быть ограничено из-за колебаний рабочих обязанностей. Подобно наименьшим привилегиям, разрешение на доступ к файлам является средством управления доступом для привилегированных пользователей в качестве модерирующего контроля [8].

Увеличение рисков

Категория «увеличение рисков» включает усиление восприятия того, что «риск обнаружения, сопротивления и задержания», связанный со злонамеренными действиями, будет высоким. Его подкатегории включают следующее: продление опеки; помощь в естественном наблюдении; снижение анонимности; усиление формального надзора.

Контроль информационной безопасности, предлагаемый для расширения опеки, предполагает управление мобильными объектами [3]. Цель управления «Мо-

бильные вычисления и удаленная работа» из ISO/IEC 27002 является более всеобъемлющей, поскольку она обеспечивает соблюдение политик удаленного доступа через мобильные устройства и сотрудников, которые работают удаленно (т.е. удаленная работа) [9].

Средства управления информационной безопасностью, рекомендуемые для естественного наблюдения, включают отчеты об инцидентах [10] и средства визуализации. Капелли и др. [12] утверждают, что отчетность об инцидентах сама по себе недостаточна, и настаивают на том, что должен быть конкретный план реагирования на инсайдерские инциденты. Средства управления информационной безопасностью, которые рекомендуются для снижения анонимности, включают контрольные журналы и регистрацию событий [3]. В частности, предлагаются контрольные журналы и журналы событий, которые полностью защищены от несанкционированного доступа, поскольку инсайдеры вполне могут подделывать контрольные журналы, чтобы скрыть свое вредоносное поведение.

Техника использования менеджеров предполагает размещение сотрудников, которые естественным образом контролируют окружающую среду в качестве сдерживающего фактора [13]. Методы информационной безопасности, предложенные для использования менеджерами по месту, включают в себя регистрацию двумя людьми [3], мониторинг использования ресурсов [14] и конкретное назначение обязанностей по информационной безопасности (IS) [8]. Подписание двумя лицами поможет снизить риск вымогательства. Конкретное распределение обязанностей является еще одной полезной стратегией, поскольку процесс может быть более информативным, если конкретные лица будут нести ответственность за свое поведение.

Для усиления формального надзора рекомендуются следующие средства контроля: обнаружение вторжений [3]; управление изменением; инструменты управления конфигурацией; горячая линия для сотрудников [8]. Существует вероятность того, что системы обнаружения вторжений могут быть нечувствительны к командам, отдаваемым злоумышленником, и такие команды могут казаться частью его/ее обычных обязанностей, поэтому тревога не будет поднята. Введение горячей линии для сообщения о подозрительном поведении [8] может помочь в раннем обнаружении. Кроме того, формальное наблюдение можно усилить, введя контроль изменений и управление конфигурацией — первое обеспечит надлежащее управление всеми изменениями, внесенными в сеть, а второе позволит обнаружить изменения в исходном коде и файлах приложений [12].

Уменьшение вознаграждения

Категория «уменьшение вознаграждение» включает в себя снижение восприятия того, что выгоды от преступления [13] будут иметь смысл. Примеры таких методов включают следующее: сокрытие целей; удаление целей; идентификация собственности; отказ в льготах. Стратегия сокрытия целей включает ограничение, по мере возможности, публикации общедоступной информации. Был предложен более широкий термин, а именно «безопасность через неизвестность». Безопасность за счет неясности — полезная техника, так как она создает препятствия на пути потенциальных злоумышленников, однако она должна быть дополнена другими средствами контроля.

Удаление целей — это родственный метод, который включает в себя затемнение целей путем развертывания элементов управления Clear Desk и Clear Screen, как рекомендовано стандартом ISO/IEC 27002 [9]. Введение изоляции конфиденциальной системы может быть дополнительным средством защиты особо конфиденциальной информации от внутренних угроз, поскольку это снижает доступность системы [8] (также рекомендуется для «целевой защиты» Коулз-Кемп и Теохариду [10]).

Водяные знаки [14], цифровые подписи [3] и классификация информации [14] рекомендованы в качестве стратегий информационной безопасности, эквивалентных технике идентификации собственности. Однако водяные знаки становятся неэффективными, если у инсайдера есть доступ к исходному объекту. Хотя цифровые подписи могут оказаться полезными для подтверждения авторства, они требуют дополнительной проверки, такой как метки времени. Вместо простой классификации информации управление активами (ISO/IEC 27002) было предложено в качестве инструмента для идентификации собственности, поскольку оно более всеобъемлющее и включает в себя учет активов [9].

Шифрование [3], механизмы автоматического уничтожения данных [14], управление непрерывностью [10] и управление инцидентами [10] предлагаются в качестве методов информационной безопасности, которые дают результаты, аналогичные методу «отказ от преимуществ». Автоматическое уничтожение данных механизмами, которые мгновенно уничтожают конфиденциальные данные, снижает вероятность их похищения. «Управление непрерывностью бизнеса» и «Управление инцидентами информационной безопасности» — это пункты стандарта ISO/IEC 27002 [9], а сравнительный контроль в COBIT — это «Управление запросами на обслуживание и инцидентами» и «Управление непрерывностью». Элементы управления «Управление за-

просами на обслуживание и инцидентами» включают минимизацию сбоев за счет быстрого разрешения инцидентов, а «Управление непрерывностью» включает реагирование на инциденты для продолжения критически важного бизнеса [15].

Уменьшение провокаций

Категория «снижение провокации» включает удаление «вредных раздражителей из окружающей среды» [13], что может спровоцировать преступление. В этой категории рассматриваются ситуации, которые действуют как триггеры или катализаторы для человека, который уже мотивирован [12]. Подкатегории включают: уменьшение разочарований и стресса; избежание споров; снижение эмоционального возбуждения; нейтрализация давления со стороны сверстников и предотвращение подражания.

Создание благоприятной рабочей среды [10] было предложено в качестве общей методики для уменьшения фрустрации и стресса. Необходимо применять конкретную технику для работы с этой категорией, основанной на выявлении «болевых точек и триггерных событий». Примерами болевых точек являются потеря данных, отказ в обслуживании и использование новых технологий, а примерами триггеров являются новые правила и технологические изменения. Уиллисон [3] рекомендует включать поддержку осведомителей в подкатегорию «содействие естественному наблюдению»; однако, поскольку предполагалось, что этот метод влияет на эмоциональные реакции на провокацию, он был переведен в категорию «снижение провокаций». Споров можно избежать или разрешить, просто внедрив План разрешения споров для эффективного управления спором.

Коулз-Кемп и Теохариду [10] рекомендуют безопасность использования и участие пользователей в процессе анализа рисков в качестве возможных средств защиты информации для снижения эмоционального возбуждения. Участие пользователей в целом было бы полезным, поскольку внутренние угрозы могут возникать, когда политики безопасности или средства контроля неправильно понимаются, плохо сообщаются или применяются непоследовательно. Внутренние угрозы также могут возникать в результате отсутствия процедурной справедливости. Поэтому может быть полезно привлекать пользователей на протяжении всего жизненного цикла информационной безопасности, от разработки до внедрения. Удобство использования системы безопасности может стать шагом на пути к уменьшению отрицательной реакции инсайдера на средства управления информационной безопасностью.

Устранение оправданий

Категория «убрать оправдания» предполагает нейтрализацию моральных убеждений преступника [13]. Преступники склонны оправдывать свое преступление. Например, инсайдеры могут рационализировать свои действия, считая киберпреступность преступлением без потерпевших. Подкатегории включают правила установки; инструкции по размещению; содействие соблюдению требований; пробуждение совести и контроль над наркотиками и алкоголем.

Что касается подкатегории «установление правил», правила устанавливаются в отношении типичных политик, соглашений и процедур, которые были предложены (например, такие процедуры, как политика приемлемого использования [8]). Хиндуджа и Коой [8] также предлагают внедрить программу помощи, чтобы помочь сотрудникам быть осведомленными об этих правилах и процедурах. Единый вход [3]; этически обоснованная деловая практика [8]; единая точка отсчета для безопасности [10] и продвижение здоровой рабочей среды [8] были предложены в качестве средств управления информационной безопасностью для реализации метода, направленного на содействие соответствию. Единый вход предполагает, что инсайдер получает один пароль во всех системах; это способствует удобству использования и может управляться централизованно. Единый вход считается аспектом «централизованного управления пользователями», который также был включен в оценку. Это понятие распространяется на метод «единой точки отсчета безопасности», который включает централизованное управление политиками информационной безопасности. Хиндуджа и Коой [8] предполагают, что продвижение здоровой окружающей среды, а также этически обоснованной деловой практики представляет собой стратегию, способствующую соблюдению организационных политик и процедур. Такая стратегия не только снижает возможность для индивидуумов заниматься преступным поведением, но и побуждает к нормативному поведению.

Средства защиты информации, рекомендуемые для обращения к совести пользователей, включают защиту авторских прав [10]; кодекс этики [10]; предупреждающие сообщения при входе в систему [8] и контекстно-зависимые интерфейсы. В COBIT проводится различие между организационной этикой и индивидуальной этикой [15]. Это означает, что организации должны учитывать личную этику при рассмотрении этического кодекса организации. Согласно Хиндуджа и Коой [8], полезно получать предупреждающие сообщения при входе в систему, поскольку такие сообщения угрызают совесть пользователя.

Хотя «контроль над наркотиками и алкоголем» может показаться несовместимым с областью информационной безопасности, общепризнано, что злоупотребление наркотиками и алкоголем ухудшает суждение инсайдера. Исследование, о котором в настоящее время сообщается, последовательно предлагает программу реабилитации сотрудников. Хиндуджа и Кооой [8] предлагают ввести процедуры для рассмотрения жалоб и предоставления адекватных льгот работникам, поскольку, по их мнению, такие меры контроля служат для утверждения пользователей и предотвращения чувства дискриминации.

Заключение

Данная статья вносит два важных вклада в понимание и снижение внутренних угроз. Во-первых, приведенная здесь информация может использоваться в качестве упреждающей стратегии смягчения действий инсайдеров. Эта оценка может быть использована для реализации средств управления информационной безопасностью, которые должны дать возможность администраторам информационной безопасности предотвращать и, возможно, противодействовать внутренним угрозам. Во-вторых, было выявлено несколько потенциальных направлений исследований. Выявленные пробелы требуют более глубокого изучения.

Некоторые результаты текущего исследования вызывают разногласия в том смысле, что популярные инструменты, такие как антивирусы, управление инцидентами и системы предотвращения утечек данных (DLP) были оценены плохо. Возможная причина может заключаться в том, что, хотя эти методы полезны, они не решают проблему внутренних угроз напрямую. Установлено также, что управление инцидентами, включающее в себя восстановление систем после инцидента, вероятно, не играет роли в обнаружении или предотвращении инсайдерской атаки. Не исключено, что инсайдеры, причастные к угрозе, входят в состав группы реагирования на инциденты.

Категории затрат и выгод, такие как «увеличение усилий», «увеличение риска» и «уменьшение вознаграждения», заставляют рационального инсайдера вычислить чистую стоимость преступления. С другой стороны, категории «устранение оправданий» и «уменьшение количества провокаций» являются косвенным контролем, который заставляет инсайдера рассматривать возможность совершения преступления с рациональной точки зрения, не руководствуясь провокациями или оправданиями. Возможно, что наличие меньшего количества элементов управления в пределах определенной категории может повысить уязвимость организации. Текущий набор методов информационной безопасности явно недостаточен для борьбы с внутренними угрозами, поскольку при их разработке не учитывались соображения, ограничивающие возможности. Необходимо провести дальнейшие исследования не только для разработки более эффективных инструментов для каждой категории, но и для определения соотношения инструментов, необходимых для каждой категории, чтобы эффективно минимизировать внутренние угрозы.

ЛИТЕРАТУРА

1. CSO MAGAZINE, USSS, CERT, Deloitte, 2011 Cybersecurity Watch Survey: organizations need more skilled cyber professionals to stay secure. [Электронный ресурс]. — URL: www.cert.org/archive/pdf/CyberSecuritySurvey2011.pdf (дата обращения 01.03.2023).
2. IT Governance, Boardroom Cyber Watch 2013: report. [Электронный ресурс]. — URL: www.itgovernance.co.uk/what-is-cybersecurity/boardroom-cyber-watch.aspx (дата обращения 01.03.2023).
3. R. Willison, Understanding the perpetration of employee computer crime in the organisational context, Information and Organization 16 (4) (2006) 304–324.
4. K. Padayachee, A conceptual opportunity-based framework to mitigate the insider threat, Information Security for South Africa, Johannesburg, South Africa, August 2013.
5. M. Theoharidou, S. Kokolakis, M. Karyda, E. Kiountouzis, The insider threat to information systems and the effectiveness of ISO17799, Computers & Security 24 (6) (2005) 472–484.
6. D.B. Cornish, R.V. Clarke, Opportunities, precipitators and criminal decisions: a reply to Wortley's critique of situational crime prevention, Crime Prevention Studies 16 (2003) 41–96.
7. S.T. Mansfield-Devine, The promise of whitelisting, Network Security 7 (2009) 4–6.
8. S. Hinduja, B. Kooi, Curtailing cyber and information security vulnerabilities through situational crime prevention, Security Journal 26 (4) (2013) 383–402.
9. ISO/IEC 27002:2005, Information technology — security techniques — information security management systems — code of practice for information security management. [Электронный ресурс]. — URL: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297 (дата обращения 01.03.2014).
10. L. Coles-Kemp, M. Theoharidou, Insider threat and information security management, in: C.W. Probst, J. Hunker, D. Gollmann, M. Bishop (Eds.), Insider Threats in Cyber Security, Springer, US 2010, pp. 45–71.
11. K. Padayachee, A framework of opportunity-reducing techniques to mitigate the insider threat: towards best practice, Information Security for South Africa (ISSA), Johannesburg, South Africa, August 2015.

12. M. Cappelli, A.P. Moore, T.J. Shimeall, R. Trzeciak, Common sense guide to prevention/detection of insider threats. [Электронный ресурс]. — URL: https://www.cylab.cmu.edu/files/pdfs/CERT/CommonSenseInsiderThreatsV2.1–1–070118–1.pdf 2006 (дата обращения 01.03.2023).
13. T.R. Smith, J. Scott, Policing and crime prevention, in: D.A. Mackey, K. Levan (Eds.), Crime Prevention, 1st ed.Jones & Bartlett, Burlington, Massachusetts 2011, pp. 61–88.
14. N.L. Beebe, V.S. Roa, Using Situational Crime Prevention theory to explain the effectiveness of Information Systems Security, Paper Presented at the Proceedings of the 2005 SoftWars Conference, Las Vegas, Nevada, December 2005.
15. ISACA, COBIT Five: For Information Security, Information Systems Audit, & Control Association, USA, 2012.

Журнал «Современная наука: актуальные проблемы теории и практики»

Финансовый университет при Правительстве РФ