STIX объединит всех киберзащитников

Об авторе:

Алексей Лукацкий, бизнес-консультант по безопасности, Cisco Systems

Stuxnet, Duqu, Flame, Red October… все это кибератаки, которые высветили совершенно новую проблему в рамках международной информационной безопасности (МИБ). Если раньше из трех аспектов МИБ (кибервойны, киберпреступность и кибертерроризм) деятельность почти всех государств крутилась вокруг борьбы с киберпреступностью, то в 2010 г. стало ясно, что кибервойны и кибероружие – уже не просто сюжет фантастического фильма; это реальность с которой нам предстоит иметь дело в ближайшее время. При этом усилия политиков и дипломатов по принятию международных конвенций по нераспространению кибероружия пока не увенчались успехом. Но с нарастающей угрозой надо что-то делать. Традиционные меры борьбы с киберпреступностью и кибервойнами уже не так эффективны. Необходим совершенно иной уровень взаимодействия между всеми участниками этой битвы.

Понимая это, 28 декабря 2012 г. президент Путин на своей встрече в Кремле с офицерами, назначенными на высшие командные должности, заявил, что нужно продолжать действовать "*системно и наступательно, в том числе по таким направлениям, как контрразведка, защита стратегической инфраструктуры, борьба с преступлениями в сфере экономики, в киберпространстве*". Это, пожалуй, один из первых случаев, когда глава государства публично заявил о новых приоритетах для отечественных спецслужб.

Буквально на следующий день, 29-го декабря, Владимир Путин подписывает указ №1711 об изменении состава Межведомственной комиссии Совета Безопасности РФ по информационной безопасности. Основным изменением стало появление в ее составе ответственных за безопасность лиц Роснефти, Росатома и Газпрома, т.е. трех отечественных стратегических инфраструктур, кибератаки на которые могут привести к достаточно печальным последствиям для экономики и национальной безопасности страны.

А спустя всего две недели 15 января 2013 г. Президент России подписал еще один документ - Указ №31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ». Все полномочия по созданию данной системы, разработке методики обнаружения атак, обмену информацией между госорганами об инцидентах ИБ, оценке степени защищенности критической информационной инфраструктуры возложены на ФСБ. В совокупности с

«Основными направлениями государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации», выпущенными Советом Безопасности летом 2012-го г., выглядят все эти действия как реализация целенаправленной программы по защите отечественных критических информационных инфраструктур от атак из киберпространства.

Однако за стратегией должны стоять вполне конкретные шаги, реализующие описанный в 31-м Указе план действий, чем Россия пока не может похвастаться. В 2000-м году я написал первую в России книгу, посвященную системному исследованию вопросов обнаружения и реагирования на компьютерные атаки, и с тех пор не выпускал из внимания эту тему. Могу с определенной уверенностью утверждать, что пока у нас нет инструментов реализации, описанных в Указе №31с. Одним из таких инструментов является «*обмен информацией между федеральными органами исполнительной власти о компьютерных инцидентах, связанных с функционированием информационных ресурсов Российской Федерации*» и «*обмен информацией между федеральными органами исполнительной власти и уполномоченными органами иностранных государств (международными организациями) о компьютерных инцидентах, связанных с функционированием информационных ресурсов*», порядок которых должна определить ФСБ. Пока такой порядок отсутствует.

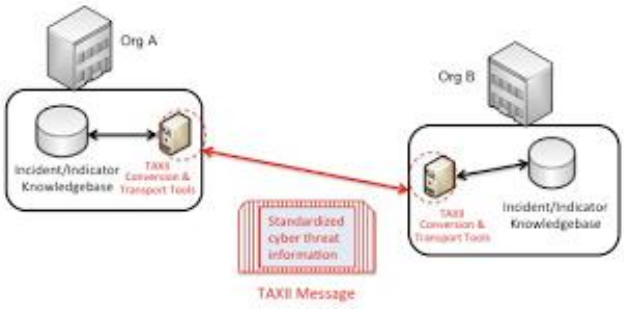
12 февраля 2013 г. президент США Барак Обама также подписал указ, похожий на Указ Президента РФ 31с, который получил название «Усиление кибербезопасности критических инфраструктур». Он продолжил последовательно реализуемую последние годы стратегию американских ведомств по повышению уровня защищенности американских критических инфраструктур. Данный указ состоит из 6-ти направлений, которые будут реализовываться различными агентства и федеральными структурами, одним из которых также является обмен информацией о киберугрозах.

Мы видим, что и США и Россия стоят перед одинаковыми задачами не только внутри государства, но и на межгосударственном уровне. Существует ли инструмент, облегчающий решение данной задачи? Оказывается да. Им может стать протокол **STIX** (Structured Threat Information eXpression). Инициатором его разработки стала американская корпорация MITRE, широко известная на ниве стандартизации вопросов обеспечения информационной безопасности. Именно она является автором широко известного и ставшего стандартом де-факто механизма именования и оценки уязвимостей CVE (Common Vulnerability Evaluation). MITRE «шефствует» и над другими стандартами, которые предназначены для решения насущных задач, стоящих перед специалистами по информационной безопасности – обмен информацией об уязвимостях, оценка рисков уязвимостей, язык описания уязвимостей и т.д. (OVAL, CCE, CEE, CME, CWE, CPE, CRF, CAPEC, SCAP, CVSS и XCCDF). Но если все эти стандарты были ориентированы в первую очередь на управление уязвимостями, то STIX направлен на *обмен информацией* об угрозах.

Нельзя сказать, что раньше такого обмена не было. Каждое ведомство или компания использовали какие-то собственные наработки, непозволяющие эффективно коммуницировать между собой. Ни о какой стандартизации и речи не шло. И если такие проблемы возникали на уровне межведомственного обмена внутри одной страны, то что говорить о межгосударственном сотрудничестве? В условиях же появления совершенного нового класса угроз – APT (Advanced Persistent Threats), задача оперативного обмена информацией о них стала как никогда актуальной. Идея STIX достаточно проста - этот протокол должен устранить вышеназванный недостаток.

Он позволяет унифицировать описание различных угроз и связанных с ними параметров - индикаторы атаки, информация об инциденте, используемый для атаки инструментарий или уязвимости, предполагаемые меры нейтрализации атаки, информация о предполагаемом противнике/нарушителе, а также о его тактике, используемой технике и процедурах, кампания, в рамках которой осуществляется атака (например, Red October) и т.п. Но STIX только стандартизует описание угроз, но не отвечает на вопрос, как обмениваться информацией о них? Эту задачу решает второй протокол, разработанный MITRE в паре со STIX – протокол TAXII, который и унифицирует способы обмена информации об угрозах, описанных с помощью STIX.

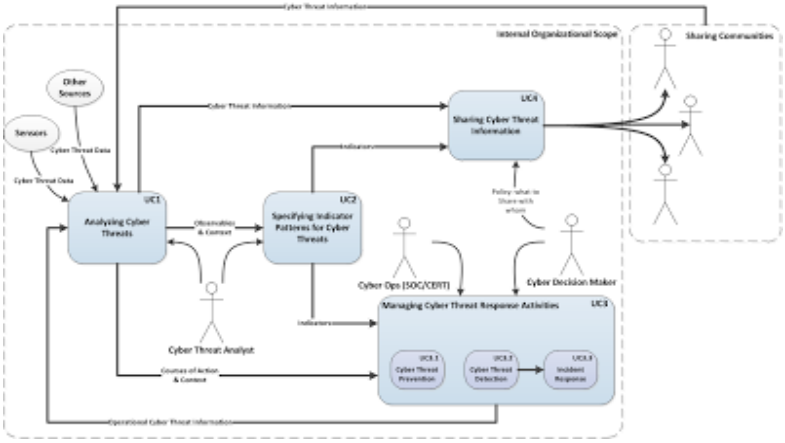
Иллюстрация 1. Схема протокола TAXII (нажмите, чтобы увеличить).



В целом, картина выглядит достаточно логично и целостно. И очень удачно она ложится на задачу, поставленную Указом Президента №31с. Есть аналитики ФСБ, которые проводят анализ угроз и прогнозируют изменение их ландшафта. Есть большое количество органов исполнительной власти, являющихся как мишенями для кибератак, так и источниками информации об угрозах для аналитиков ФСБ. Есть методика ликвидации последствий атак. Есть инфраструктура обмена информацией между органами власти. А протоколы STIX и TAXII дают возможность автоматизировать процесс обмена информацией между всеми вышеперечисленными элементами.

Но только ли для реализации Указа №31с подходит STIX? К счастью, нет. В РФ у этого стандарта могут быть неплохие перспективы. Во-первых, в России существует несколько центров реагирования на компьютерные угрозы (CSIRT), для которых задача обмена информацией об угрозах вполне актуальна. Например, Центр реагирования на компьютерные инциденты в информационных системах органов государственной власти Российской Федерации(GOV-CERT.RU), созданный 8-м центром ФСБ.

Иллюстрация 2. Схема протокола STIX (нажмите, чтобы увеличить).



Но GOV-CERT.RU не единственная в России структура, которая занимается реагированием на инциденты. Согласно последнему отчету европейского агентства по сетевой безопасности ENISA в нашей стране таких организаций (исключая новый GOV-CERT) всего три - CERT-GIB, WebPlus ISP и RU-CERT. Первый из этой тройки был создан совсем недавно. Его основатель - компания *Group-IB*. Этот CERT - сугубо частный центр реагирования, обслуживающий сторонние организации и претендующий на звание «прогосударственного», т.к. именно с ним Координационным центром национального домена сети Интернет было заключено соглашение о противодействии киберугрозам в доменах .RU и .РФ (наряду с подразделением Лиги безопасного Интернета - фондом «Дружественный Рунет»).

Webplus ISP CERT занимается обслуживанием только собственных ресурсов, а вот RU-CERT, претендуя на звание национального CERTa, все-таки таковым не является. Хотя он является первым центром реагирования в России. Я помню, в Ассоциации документальной электросвязи (АДЭ) мы эту инициативу РОСНИИРОСа обсуждали много лет назад. Однако за эти годы RU-CERT никакой активности не проявлял и я о ней не слышал (хотя это не доказывает, что ее не было).

Вторым местом, где стандарт STIX был бы очень полезен, является создаваемый Национальный центр борьбы с преступлениями в платежной сфере. О его создании уже неоднократно заявляло некоммерческое партнерство «Национальный платежный совет» (НП НПС), а саму инициативу на самом высоком уровне поддержал Банк России. Предполагается, что в числе базовых функций создаваемого центра станут информационная, консультационная и юридическая поддержка участников Национальной платежной системы по противодействию мошенничеству с денежными средствами, создание и поддержание в актуальном состоянии базы данных организаций и физических лиц, в том числе, участников Национальной платежной системы, уличенных в мошеннических действиях, ряд других задач. Очевидно, что одним из инструментов функционирования данного Центра должен стать обмен информацией и STIX тут подходит как нельзя лучше.

Развивая тему применения STIX в финансовой сфере нельзя не сказать об инициативе российских властей о создании в Москве Международного финансового центра (МФЦ), в деятельности которого вопросы обмена информацией об угрозах с другими аналогичными международными центрами были бы весьма актуальными.

Остается только простой вопрос – как сделать так, чтобы стандарт STIX стал применяться в России? Ведь пока это инициатива частной американской компании, а в России (как минимум, в государственных проектах) существует определенное недоверие ко всему, что исходит с той стороны океана. Именно поэтому так важно для указанного протокола получить международную поддержку со стороны соответствующих организаций по стандартизации. Ими могут стать IETF или ITU. Хотя не исключено, что мы опять будем изобретать велосипед и разрабатывать собственные протоколы взаимодействия. Вопрос пока остается открытым.

Материал подготовлен специально для электронного бюллетеня ПИР-Центра Пульс Кибермира.