Готовность России к ведению современных кибервойн

Рустэм ХАЙРЕТДИНОВ,
генеральный директор компании «Атак Киллер»

Сегодня многие государства объявляют о создании подразделений для ведения кибервойны, как и принято в политике, убеждая всех окружающих, что в их планах исключительно оборона от нападения в киберпространстве. Когда все обороняются, непонятно, кто же тогда нападает, – довольно сложно сегодня представить, что два или более государств открыто столкнутся в киберпространстве.

Кибернападение

Под нападением в кибервойне сейчас подразумеваются скорее действия не штатных киберармий, а хакерских группировок, возможно, подконтрольных государствам (непонятно каким) или нанятых корпорациями, политизированных кибертеррористических групп либо правительственных и корпоративных разведок. Все они по-разному мотивированы, по-разному организованы и могут выступать за разные стороны конфликта последовательно или даже одновременно. Хакерские группировки больше подходят для грабежа или вымогательства, кибертеррористы, как и террористы обычные, нацелены на отдельные акции в политических целях, корпоративные и государственные разведки нацелены на скрытые операции по похищению информации с последующим оглашением либо без него.

Кибервойна в значении «война», т. е. объявленное и открытое противостояние двух и более государств, сегодня вряд ли возможна – таким образом она быстро перерастет в настоящую, горячую войну, а при участии в ней ядерной державы – и в ядерную. Однако невозможность открытой войны не исключает отдельных актов нападения всех типов, скорее всего, от неизвестного противника, что делает актуальной необходимость наращивать не только защиту отдельных государственных объектов или частных объектов государственной важности, но и всю информационную инфраструктуру страны в целом.

Критическая инфраструктура

Сегодняшнюю критическую информационную инфраструктуру в России можно условно разделить на два вида: старую и новую. Старая инфраструктура – оставшаяся с условно «советских» времен: закрытые информационные системы, проприетарные протоколы, часто российской разработки. Такая инфраструктура характерна для промышленных систем повышенной опасности: электростанций, включая атомные, транспортных систем, металлургических и нефтеперерабатывающих заводов. Информатизация последних 20 лет не затронула ключевую архитектуру этих систем, проникнув только на уровень коммуникаций и документооборота. Безопасность в таких системах встроена в архитектуру и часто не требует отдельных навесных систем информационной безопасности.

«Новая» инфраструктура – информационные системы, построенные или полностью перестроенные в последние 20 лет: финансовые структуры, телекоммуникации (прежде всего мобильная связь и Интернет), городское управление (светофоры, «умные» здания), государственные услуги. Эти системы построены уже на новых принципах, активно используют персональные компьютеры с операционной системой Windows и Интернет, построены полностью на иностранных, чаще всего американских решениях. Создавались они в режиме жесткой экономии, использовали дешевые тиражируемые компоненты на процессорах Intel. На тот момент цена была важней, чем

безопасность, поэтому применялись не надежные, но массовые решения. Сейчас мы пожинаем плоды такой экономии: большинство успешных атак на «новую» инфраструктуру связаны с уязвимостями протоколов Интернета и операционных систем, изначально создававшихся для домохозяек.

Стоит признаться, что именно благодаря постоянным атакам на «новую» инфраструктуру сегодня корпоративные системы защищены лучше, чем государственные: до последнего времени интереса их атаковать было гораздо больше и защитники информационных систем накопили немалый опыт. Взламывать банки было выгоднее, чем государственные информационные системы, которые не содержали «монетизируемой» информации, да и возможности корпораций в найме и удержании специалистов в информационной безопасности не сравнимы с государственными.

Однако за последние несколько лет российское государство заметно продвинулось в ИТ, перенеся в информационное пространство многие государственные услуги на «новой» архитектуре. Это совпало с появлением и быстрым ростом движения «хактивистов» – политически мотивированных хакеров, нацеленных на достижение политических (добыча компромата на государственных деятелей) или террористических (вывод из строя значимых объектов) целей. Стоят ли за хактивистами государства или государственные хакеры действуют, маскируясь под вольных хакеров, – часто обсуждаемый вопрос, но в киберпространстве атрибуция атак – непростое дело и предъявляемые общественности «доказательства» заказчиков враждебных акций не выдерживают никакой критики.

Кибероборона

Так или иначе, сегодня государственные системы подвергаются атакам все чаще, при этом интенсивность атак на частный сектор экономики не снижается. Возникает серьезная проблема с кадрами: государственные информационные системы усложняются, важность находящейся в них информации возрастает, как и вариативность атак, однако по зарплатам госпредприятия обычно значительно уступают частным компаниям, особенно в интернет-холдингах, розничных банках, нацеленных на обслуживание клиентов через Интернет, на предприятиях электронной коммерции и т. п. В условиях хронической нехватки специалистов существуют два подхода к относительно быстрому (по сравнению с «нарожать и выучить») решению проблемы: концентрация специалистов в одном месте и оказание аутсорсинговых услуг или ускоренная роботизация защиты. Оба подхода имеют свои очевидные преимущества и недостатки, но их обсуждение выходит за рамки статьи.

Сегодня государственные системы подвергаются атакам все чаще, при этом интенсивность атак на частный сектор экономики не снижается.

Пожалуй, единственным открытым противостоянием государств в киберпространстве может быть отключение России от каких-то сервисов или вообще от Интернета в виде санкций: Интернет фактически контролируется из США, там же находятся многие производители компонентов информационных систем – процессоров, операционных систем, прикладного программного обеспечения, компиляторов и т. п. Такие санкции довольно долго действовали против Ирана, и страна была практически выключена из мирового обмена информацией. В 2014 г. мы уже столкнулись с отказом в обновлении и обслуживании ключевых систем, построенных на американском программном обеспечении, для российских компаний, которые вошли в санкционные списки, и наблюдаем это каждый день в Крыму. Такая угроза вполне реальна, особенно на вновь поднявшейся в США волне голословных обвинений России во всех грехах, поэтому решения по замещению постоянно обновляемых из-за рубежа импортных систем системами собственной разработки – одна из ключевых стратегий по защите критической информационной инфраструктуры страны.

Остальные виды атак – взломы информационных систем в целях похищения данных или выведения этих систем из строя, перехват управления с целью повлиять на работу критических систем и т. п. – скорее всего, будут вестись тайно и под прикрытием хакерских группировок. Они будут локальны и направлены на отдельные объекты, поэтому отражать их придется не кибер-армии страны, а штатным защитникам конкретной информационной системы.

Кибератаки могут поддерживаться также информационными атаками в соцсетях и СМИ, особенно в финансовом секторе. Достаточно вспомнить атаки на банковскую систему страны в конце 2014 г., когда кибератаки усиливались паническими слухами о конкретных банках. Такие комбинации кибер- и информационных атак вызывают

самоподдерживающиеся атаки: сначала кибератакой подавляется сайт банка, затем распространяются слухи о проблемах, клиенты банка идут проверять состояние счета и не могут этого сделать, звонят в колл-центр, слышат: «время ожидания – 80 минут», бегут в отделение и видят там очередь таких же обеспокоенных вкладчиков. После этого они публикуют скриншоты и фотографии в соцсетях, на эти публикации ссылаются уже обычные СМИ, и спираль паники от многочисленных публикаций, подтверждающих панические настроения, закручивается еще сильнее. Нагрузка на сайт и колл-центр растет, они не успевают обрабатывать сообщения, вкладчики нервничают, в отделениях очереди, банкоматы опустошаются, банк стремительно лишается резервов и приближается к банкротству. Поэтому такие атаки необходимо отражать не только собственными силами, но и с привлечением государственных сил информационного противодействия.

Кибервойна

Готова ли Россия к кибервойне? К полномасштабной, в противостоянии с США – скорее всего, нет. Стратегия в случае глобального нападения или отключения: переход на замкнутую информационную систему внутри страны без возможности влияния на нее извне. Учения по отключению российского сегмента Интернета от мировой сети проводились Минкомсвязью РФ, так что этот сценарий уже отрабатывается на практике, а значит, рассматривается правительством как вероятный.

Однако, как было отмечено, полномасштабная и открытая кибервойна с ядерной державой маловероятна – риск ее эскалации до военного конфликта без приставки «кибер» слишком велик.

> Позиция государства однозначно показывает, что защита критической информационной инфраструктуры страны – не личное дело владельцев частных объектов и их команд информационной безопасности.

А вот к локальным «боям» страна готова гораздо лучше. Большинство команд защитников информационной инфраструктуры уже прошли крещение серьезными атаками: мощные DDoS, «шифровальщики», целевые атаки, связанные с использованием фишинга и социальной инженерии. Крупные компании, чей бизнес жизненно связан с информационными технологиями, сами проводят масштабные учения, имитирующие нападение (Redteam), запускают массовое тестирование своих систем на уязвимости (bugbounty), подразумевающее выплату больших премий за обнаруженные бреши в защите. Поскольку атаковать такие системы будут не всей мощью иностранного государства, а хакерскими группами, то защита вполне адекватна угрозе.

Принятый 19 июля Закон «О безопасности критической информационной инфраструктуры Российской Федерации» наконец-то обозначил позицию государства в этой области. Причем обозначил в самой жесткой из предложенных форм – приравняв многие данные и процессы к государственной тайне, со всеми вытекающими последствиями: лицензированием деятельности, формами допуска, возрождением «первых отделов» на предприятиях и т. п. Подзаконных актов еще нет, и многие детали пока подвержены толкованию, но основной вектор понятен: гайки в этой области будут закручены, и вольнице свободных хакеров-пентестеров систем АСУ ТП приходит конец.

Позиция государства однозначно показывает, что защита критической информационной инфраструктуры страны – не личное дело владельцев частных объектов и их команд информационной безопасности, поэтому владельцы таких объектов получат поддержку для ее обеспечения: от информационно-методической через ФинЦЕРТ и ГосСОПКА до финансовой и юридической. Впрочем, и до принятия закона МВД и ФСБ успешно занимались расследованием преступлений в отношении транспортных компаний и банков, теперь эта поддержка будет усилена.

Заключение

«Хочешь мира – готовься к войне», – гласит древняя латинская пословица. Мы все надеемся на то, что киберпространство не станет ареной полномасштабных войн, но если все стороны будут хорошо подготовлены к такой войне и ни одна не будет иметь стратегического перевеса, то смысла в такой войне не будет. Укрепляя обороноспособность страны в целом и в том числе ключевых элементов инфраструктуры (финансы, транспорт, промышленность, энергетика, госуправление), замещая базовые решения решениями собственного производства, мы уравновешиваем силы в потенциальном противостоянии и уменьшаем вероятность чреватого «горячей войной» полномасштабного конфликта в киберпространстве. ■