Охват всего периода атаки: до, во время и после

Пора подумать о новой модели информационной безопасности

Современный ландшафт угроз сильно отличается от того, что мы наблюдали всего 10 лет назад. Простые атаки, причиняющие ограниченный ущерб, уступили место современной киберпреступности — изощренной, хорошо финансируемой и способной вызывать крупные сбои в работе компаний и государственных учреждений. Эти новые виды атак не только менее заметны, но и дольше задерживаются в сетях. Они также способны накапливать сетевые ресурсы для увеличения радиуса действия.

Традиционные методы защиты, которые полагаются лишь на обнаружение и блокирование атак, больше не эффективны. Пришло время для новой модели информационной безопасности, в которой учитывается весь период атаки — до, во время и после.

Коммерциализация хакерства

Первые компьютерные вирусы появились более 25 лет назад. Едва ли мы понимали, что это было лишь начало, после которого хакерство превратится в хорошо отлаженный бизнес.

Почти 10 лет вирусы оставались основной угрозой, и со временем были созданы способы защиты от них. Поэтому хакеры, узнавая о новых видах уязвимостей, продолжали изобретать новые виды атак. Это была, так сказать, гонка вооружений, в которой одни создавали угрозы, а другие учились от них защищаться. Приблизительно каждые пять лет хакеры запускали в ход новые виды угроз: от макровирусов до программных червей, шпионского ПО и руткитов. Специалисты, в свою очередь, разрабатывали методы для защиты сетей.

Неудивительно, что мы можем соотнести эти циклы с важнейшими технологическими скачками, которые определяли новые направления атак (см. рис 1). Первые вирусы по большей части были нацелены на операционную систему и распространялись благодаря «сети с посыльными». Жертвами макровирусов становились пользователи, обменивающиеся файлами. Программные черви, которые «переползали» между компьютерами, действовали благодаря корпоративным сетям и растущей популярности Интернета. Шпионское ПО и руткиты возникали с появлением новых приложений, устройств и веб-сообществ. Сегодня мы противостоим новым видам вредоносного ПО, направленным угрозам и изощренным атакам постоянного действия (APT). Изменились мотивы злоумышленников и средства, используемые в атаках. Так современные угрозы гораздо сложнее заметить, понять и остановить.

Рисунок 1. Превращение хакерства в бизнес

Благодаря коммерциализации хакерства появляется более быстрая и действенная преступность, которая получает прибыль от нападения на ИТ-инфраструктуру. Организованный обмен вредоносными кодами процветает и приносит доход, а открытый рынок стимулирует переход от простой эксплуатации уязвимостей к краже информации и намеренному повреждению систем. Когда киберпреступники поняли, что они могут хорошо заработать на своем ремесле, их работа стала более упорядоченной и нацеленной на результат. Злоумышленники осознают статическую природу классических методов защиты и их изолированность, поэтому они могут использовать пробелы между зонами защиты и уязвимости в них. Нередко команды хакеров даже следят за разработкой ПО, тестируя качество или испытывая свои продукты с реальными технологиями безопасности. Такая проверка позволяет убедиться, что их вредоносное ПО сможет обойти используемые способы защиты.

Утечки важной информации несут значительные финансовые потери, и многие группы «хактивистов» запускают атаки, которые приносят экономическую или политическую выгоду с малой вероятностью наказания. Новые методы атак (переходы между портами и протоколами, зашифрованное туннелирование, файлы-носители, угрозы смешанных типов, использующие социальную инженерию, атаки нулевого дня и прочие) позволяют хакерам проще, быстрее и дешевле проникать в сеть, а защитникам становится сложнее их заметить и блокировать. Такое неуловимое вредоносное ПО само может меняться по мере продвижения по корпоративной сети в поисках надежного укрытия для извлечения критически важных данных.

Проблема универсальных коммуникаций

Современные расширенные сети и их составляющие постоянно развиваются, порождая новые направления атак. Сюда относятся мобильные устройства, веб-ориентированные приложения и приложения удаленного использования, гипервизоры, социальные сети, веб-браузеры и встроенные компьютеры, а также многие устройства и службы, о которых мы только можем догадываться, появляющиеся благодаря Всеобъемлющему Интернету. Люди работают как внутри, так и снаружи сети, на любом устройстве, получают доступ ко всем приложениям и в различных облаках. Это влечет за собой проблему универсальных коммуникаций. Хотя подобные тенденции положительно сказываются на развитии коммуникаций, они также увеличили количество точек входа и способов для взлома. К сожалению, большинство организаций не успевает разворачивать средства защиты в таком темпе.

Как правило, организации защищают расширенные сети с помощью различных технологий, которые не могут работать сообща, да и не предназначены для этого. Также они могут полностью положиться на операторов связи в вопросе информационной безопасности в облаке и на хостинги для защиты интернет-инфраструктуры. В этих новых реалиях администраторы системы информационной безопасности зачастую не имеют полного контроля над устройствами и приложениями, которые имеют доступ к корпоративной сети, а также не успевают реагировать на новые угрозы.

Новые тенденции в области информационной безопасности

Пытаясь решить проблему сочетания различных видов атак с инфраструктурой универсальных коммуникаций, специалисты по безопасности задаются тремя важными вопросами.

1. *Учитывая новые бизнес-модели и направления атак, как нам поддерживать информационную безопасность и соответствие нормативным требованиям при постоянном изменении ИТ-ландшафта?* Организациям, которые переходят к использованию облачных вычислений, виртуализации и мобильных устройств ради производительности, гибкости и эффективности, следует усовершенствовать свою инфраструктуру безопасности.
2. *Как нам обеспечить постоянную защиту от новых атак и все более изощренных угроз?* Злоумышленники не очень разборчивы: они ищут любые слабые звенья в цепи. Они сделают все, чтобы довести атаку до конца, нередко используя инструменты, которые были разработаны для выбранной инфраструктуры безопасности. Они постараются остаться незамеченными, применяя технологии и методы, которые практически не оставляют следов.
3. *Как можно одновременно решить первые две проблемы и уменьшить сложность и фрагментацию решений информационной безопасности?* Организации не могут позволить себе оставлять дыры в защите, которым будут рады современные опытные хакеры. В то же время усложнение защиты с помощью разнообразных, но несовместимых решений не обеспечит необходимый уровень безопасности.

> *«100 % компаний подключены к доменам, которые служат источниками вредоносного ПО».*
>
> – Годовой отчет Cisco по информационной безопасности за 2014 год

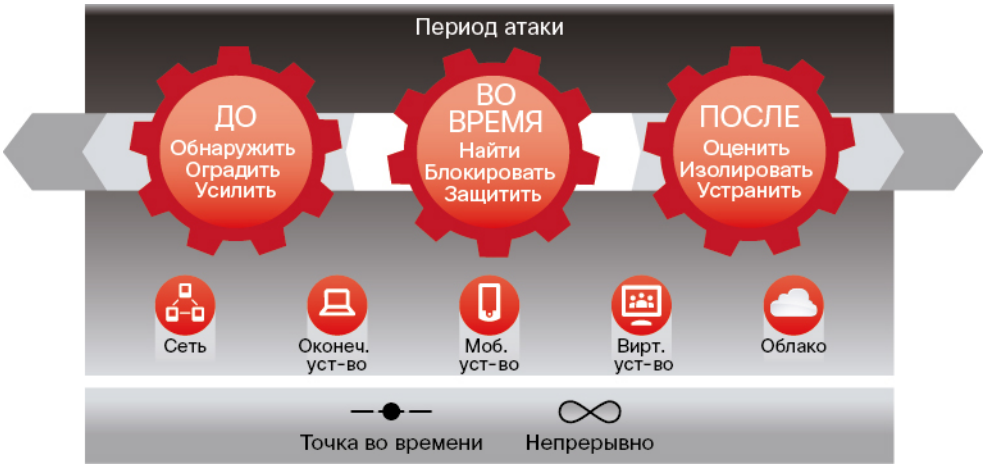
Сочетание этих тенденций (изменение бизнес-моделей, расширение ландшафта угроз, сложность и фрагментарность систем информационной безопасности) привело к появлению дыр и проблем управления безопасностью, нарушению жизненного цикла средств защиты и уменьшению прозрачности сети. Для надежной защиты организаций необходимо изменить сам подход к обеспечению информационной безопасности. Пришло время новой модели информационной безопасности, ориентированной на угрозу.

Охват всего периода атаки: до, во время и после

Современные инструменты защиты нацелены на мониторинг сети и блокирование вредоносного ПО в точке входа. Эти инструменты сразу же сканируют файлы на предмет угрозы. Однако новые атаки нельзя назвать одномоментными: они длятся долго и требуют постоянного внимания. Теперь, чтобы избежать обнаружения, злоумышленники используют тактики, среди которых переходы между портами, инкапсуляция, атаки нулевого дня, атаки «разделяй и властвуй» (C&C), боковое движение, зашифрованный трафик, смешанные угрозы и обход «песочницы». Если файл не пойман или модифицируется, становясь вредоносным после входа в среду, то технологии одномоментного обнаружения уже не смогут заметить последующие действия по развертыванию атаки.

Средства защиты должны не только уметь обнаружить угрозу, но и минимизировать вред от успешной атаки. Организациям следует провести комплексный анализ модели безопасности, улучшить прозрачность сети и контроль в течение всего периода атаки: до ее начала, во время активной фазы и даже после нанесения вреда системам и потери информации (см. рисунок 2).

Рисунок 2. Новая модель информационной безопасности



- **До:** необходима полная информация о том, что находится в расширенной сети; это поможет применить политики и средства защиты.
- **Во время**: необходима возможность непрерывно искать и блокировать вредоносное ПО.
- **После**: необходима ретроспективная система информационной безопасности, которая позволит уменьшить ущерб. Необходимо найти точку входа, определить область поражения, остановить угрозу, устранить риск повторного заражения и исправить повреждение.

До атаки

Для противостояния хорошо осведомленным злоумышленникам требуется система обеспечения безопасности с учетом контекста. Организации борются против злоумышленников, которые знают об инфраструктуре даже больше, чем специалисты, которые ее защищают. Чтобы обеспечить защиту сети еще до начала атаки, организациям нужна полная прозрачность среды, включая физические и виртуальные узлы, операционные системы, приложения, службы, протоколы, пользователей, контент, поведение сети и т. д. Защитникам необходимо выявлять уязвимые места инфраструктуры, учитывая предыдущие атаки и значимость цели. Чтобы правильно настроить средства защиты, им необходимо хорошо разбираться в том, что они пытаются защитить. Вся сеть должна быть полностью прозрачной: от оконечных устройств, почтовых и веб-шлюзов, виртуальных сред и мобильных устройств до центра обработки данных. Благодаря прозрачности сети специалисты смогут получать сигналы тревоги и принимать обоснованные решения.

Во время атаки

Непрерывные атаки длятся долго и требуют постоянной защиты. Традиционные средства защиты могут заметить атаку только в один момент времени, исходя из одной точки данных самой атаки. Такой подход не годится для новых видов атак. Вместо этого необходима инфраструктура безопасности, которая собирает и соотносит данные из расширенной сети с историческими моделями и данными глобальной системы анализа. Это позволит отличать активные атаки, извлечение данных и зондирование от обычных помех. Другими словами, необходимо перейти от принципа одного момента к непрерывному анализу и принятию решений. Если в сеть попал некий файл, сначала признанный безопасным, но затем проявивший вредоносное поведение, нужно немедленно предпринимать действия. Благодаря такому подходу в режиме реального времени специалисты по информационной безопасности могут автоматизировать применение политик, и ручное вмешательство больше не потребуется.

После атаки

Чтобы защищаться на протяжении всей атаки, организациям нужна ретроспективная система информационной безопасности. Это подразумевает работу с большим объемом данных, которая под силу не всем системам защиты. Благодаря инфраструктуре, способной непрерывно собирать и анализировать данные, а также средствам автоматизации, команды по обеспечению безопасности могут определять признаки угроз, обнаруживать вредоносное ПО, меняющее свое поведение, и устранять проблему. Таким образом даже те угрозы, которые оставались незамеченными в течение недель или месяцев, можно обнаружить, проанализировать, изолировать и устранить.

Эта модель информационной безопасности, ориентированная на угрозы, позволяет организациям активно действовать на протяжении всей атаки, по всем ее направлениям. Она обеспечивает постоянную защиту в реальном времени.

Внедрение новой модели информационной безопасности

Cisco полагает, что новая модель информационной безопасности требует от современных технологий защиты следующих важных качеств: они должны обеспечивать прозрачность сети, ориентироваться на угрозы и базироваться на платформе.

Прозрачность: администраторы информационной безопасности должны отслеживать всё происходящее. Эта возможность требует сочетания ширины и глубины (см. рисунок 3). Аспект ширины отвечает за возможность собирать данные по всем направлениям потенциальных атак, охватывающим сеть, оконечные устройства, почтовые и веб-шлюзы, мобильные устройства, виртуальные и облачные среды. Аспект глубины дает возможность соотносить эти сведения и применять их, чтобы изучить контекст проблемы, найти лучшее решение и выполнить действия как вручную, так и автоматически.

Рисунок 3. Ширина и глубина

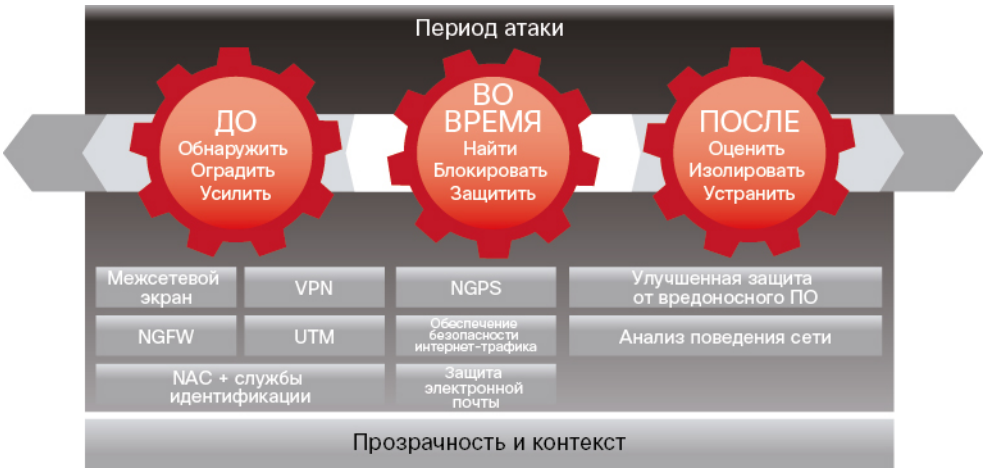
Ориентация на угрозу: современные сети работают везде, где находятся сотрудники и данные. Несмотря на значительные усилия, специалисты по информационной безопасности не всегда успевают за злоумышленниками, которые атакуют с новых направлений. Для сокращения радиуса атаки необходимы специальные политики и средства контроля, однако угрозы все равно проникают в сеть. Поэтому технологии защиты должны быть нацелены на обнаружение, анализ и устранение угроз. Ориентация на угрозы означает думать как злоумышленник, опираться на прозрачность сети и контекст для адаптации к изменениям среды и находить способ защиты от угрозы. Новое вредоносное ПО и атаки нулевого дня требуют постоянного улучшения защиты. С этой целью необходим непрерывный сбор данных облачной аналитики, которые передаются во все системы безопасности для повышения их эффективности.

На базе платформы: сейчас информационная безопасность не ограничивается сетью и требует интегрированной системы гибких и открытых платформ, которые охватывают сеть, устройства и облако. Эти платформы должны быть расширяемыми, масштабируемыми и централизованными, чтобы обеспечить унифицированные политики и средства управления. Проще говоря, они должны соответствовать масштабу атак, которые мы отражаем. Для этого необходимо перейти от устройств точечной защиты к современной платформе масштабируемых и легко развертываемых сервисов и приложений. Подход на базе платформы не только усиливает систему безопасности, устраняя уязвимости и дыры, но также позволяет быстрее обнаружить угрозу и определить защитные действия.

Охват всего периода атаки

Чтобы справиться с современными проблемами информационной безопасности и усилить защиту, организациям необходимы решения, которые действуют весь период атаки и разработаны на основе принципов прозрачности, ориентированности на угрозу и платформенности. Корпорация Cisco предлагает полный портфель решений для кибербезопасности, которые ориентированы на угрозу и действуют весь период атаки.

Рисунок 4. Охват всего периода атаки



Эти специальные решения, основанные на платформе, предлагают широчайший набор возможностей для борьбы на всех направлениях атаки. Решения работают сообща, чтобы защитить вашу сеть в течение всей атаки. Их можно интегрировать с другими программами для построения полноценной системы информационной безопасности.

- До атаки эти решения (в том числе межсетевые экраны текущего и нового поколения, средства управления доступом к сети, службы идентификации и многие другие) предоставляют специалистам безопасности инструменты, необходимые для обнаружения угроз и полноценной защиты.
- Во время атаки системы предотвращения вторжений нового поколения, а также решения для защиты почты и интернет-трафика позволяют обнаружить и блокировать вредоносные объекты, которые проникли в сеть.
- После атаки организации могут применить улучшенную защиту от вредоносного ПО, разработанную компанией Cisco, для анализа поведения сети, эффективного определения зоны поражения и устранения последствий.

Эти решения, которые можно масштабировать для поддержки даже самых крупных международных компаний, доступны всегда в виде физических и виртуальных устройств, а также облачных сервисов. Благодаря интеграции они обеспечивают прозрачность всей сети и средства контроля на всех направлениях атак.

Заключение

Превращение хакерства в бизнес и универсальные коммуникации ведут к глубоким изменениям способов защиты наших систем, заставляя нас искать новые пути решения проблем кибербезопасности. Стратегии информационной безопасности, ориентирующиеся на защиту периметра и способы предотвращения, дают злоумышленникам полную свободу действий после проникновения внутрь сети.

Сочетание этих тенденций (изменение бизнес-моделей, расширение ландшафта угроз, сложность и фрагментарность систем информационной безопасности) привело к появлению дыр и проблем управления безопасностью, нарушению жизненного цикла средств защиты и уменьшению прозрачности сети. Пришло время новой модели информационной безопасности, которая ориентируется на угрозы и обеспечивает прозрачность и полный контроль всей сети в течение всей атаки.

Только корпорация Cisco предлагает подход, который упрощает систему информационной безопасности, но в то же время обеспечивает полную прозрачность сети, непрерывный контроль и расширенную защиту от угроз в течение всей атаки. Благодаря этой новой модели информационной безопасности организации будут действовать разумнее и быстрее до, во время и после атаки.

Штаб-квартира в США
Корпорация Cisco Systems
Сан-Хосе, Калифорния

Штаб-квартира в Азиатско-Тихоокеанском регионе
Cisco Systems (USA) Pte. Ltd.
Сингапур

Штаб-квартира в Европе
Cisco Systems International BV Амстердам,
Нидерланды

Корпорация Cisco насчитывает более 200 офисов и представительств по всему миру. Адреса, номера телефонов и факсов приведены на веб-сайте Cisco по адресу www.cisco.com/go/offices.

Отпечатано в США C11-731741-01 06/14