КАК РАБОТАЕТ ПОДХОД ZERO TRUST В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Артём ТУРЕНОК
руководитель отдела технических решений АО «ДиалогНаука»

Антон ПИЛИПЕНКО
руководитель продукта Xello Datacube

Рынок кибербезопасности меняется быстрее, чем бизнес успевает адаптироваться. Компании теряют контроль над данными, сотрудники работают из дома, а в инфраструктуре — десятки, а иногда и сотни точек входа. В этих условиях традиционная модель защиты только внешнего периметра больше не работает. Это подтверждают результаты пентестов: 96% организаций оказались[1] уязвимы к внешним атакам, а в 100% случаев сотрудники получали доступ к чувствительным данным.

КОГДА СВОИ — ЭТО НОВЫЕ ЧУЖИЕ

Когда сотрудник в корпоративной сети подвергается риску — будь то удалённый сотрудник или в офисе, все меры информационной безопасности отменяются. Устройства сотрудников — новая уязвимость для специалистов информационной безопасности. 85% ИТ-специалистов считают[2], что именно действия сотрудников становятся главной причиной инцидентов — осознанных или нет. Почти треть опрошенных подтверждает, что за последние два года количество таких случаев увеличилось и продолжает расти. Причём 52% респондентов отмечают, что сотрудники не умеют распознавать[3] фишинговые письма, и в этом корень множества атак.

Корпоративные устройства (в особенности личные, BYOD) являются неконтролируемой средой, которая может хранить конфиденциальные данные, подключаемые к критически важным приложениям. Естественным решением является установка агента (применение решений класса MDM/UMM/UEM) для управления конечными точками, который решает одну проблему, но создаёт другую. Не все сотрудники готовы устанавливать подобные решения на персональные устройства, агент управляет всем устройством.

Другим подходом для контроля устройств является виртуализация рабочих мест (VDI), которая позволяет использовать личные ноутбуки и компьютеры для работы. Но эта технология имеет высокую цену, как с точки зрения стоимости лицензирования, так и с точки зрения персонала, обслуживающего её. Для удалённых пользователей, работающих в сетях с далеко не идеальными характеристиками, использование DaaS (Desktop as a Service) может быть затруднительным.

Другой вопрос, который стоит перед ИТ- и ИБ-службами — это предоставление доступа к приложениям. Для этого всё ещё используются корпоративные VPN-решения, которые основываются на модели доверия: всё, что находится внутри сети, считается надёжным и защищённым. К сожалению, злоумышленники научились использовать уязвимости, присущие VPN, что делает эту технологию серьёзной угрозой безопасности для современного бизнеса. Технология VPN расширяет внутреннюю сеть на подключённые устройства, позволяя удалённым пользователям напрямую взаимодействовать с внутренними ресурсами (обеспечивает двунаправленную связь между конечными устройствами и внутренними серверами). Таким образом, она открывает злоумышленникам возможность исследовать, сканировать и перемещаться по внутренней сети после взлома VPN.

[1] https://ptsecurity.com/ru-ru/about/news/itogi-pentestov-ot-positive-technologies-96-organizaczij-uyazvimy-pered-kibermoshennikami

[2] https://rg.ru/2024/09/17/reg-szfo/vot-tak-fokus.html

[3] https://ptsecurity.com/ru-ru/research/analytics/kakimi-budut-fishingovye-ataki-v-blizhaishem-buduschem

НА ЧЁМ СТРОИТСЯ ПОДХОД «НУЛЕВОГО ДОВЕРИЯ»

Концепция Zero Trust («нулевое доверие») предлагает кардинально другой подход, в отличие от модели, основанной на периметре, и представляет собой принципиально новую архитектуру. Эта концепция позволяет отделить безопасность и подключение к вашей сети с помощью виртуализации или контейнеризации, которая обеспечивает безопасное подключение от любого пользователя к любому сервису на границе — без предоставления доступа ко всей сети. Таким образом, модель нулевого доверия позволяет избежать чрезмерных разрешений и неявного доверия, присущих традиционным моделям подключения объектов к сети. Детальный доступ к ИТ-ресурсам с наименьшими привилегиями обеспечивается с помощью контекстно-зависимых политик, которые оценивают риски и принимают соответствующие меры.

У Zero Trust-архитектуры есть три главных принципа.

Первый — минимизация площади атаки через прямое подключение к ИТ-ресурсам и приложениям, а не сетям. Такой подход снижает риски компрометации всей сети и горизонтального перемещения для злоумышленника при взломе конечного устройства.

Второй — отсутствие доверия к пользователям и устройствам, которые проходят аутентификацию и авторизацию. Последнее предполагает допуск только тех устройств, которые зарегистрированы в системе компании, соответствуют её требованиям безопасности и находятся под контролем ИТ-службы. Авторизованные пользователи имеют доступ только к определённым приложениям, а не ко всей сети. Сегментация обеспечивает гранулярный контроль доступа.

Третий — шифрование данных как при передаче, так и в состоянии покоя. Последнее обеспечивает безопасность данных и предотвращение их использования извне (если злоумышленник получил доступ к устройству).

Подход «от пользователя к приложению», который обеспечивает концепция Zero Trust, особенно актуален для гибридной работы и распределённой инфраструктуры, позволяя цифровым экосистемам работать без прямого подключения сервисов к интернету.

РЕАЛИЗАЦИЯ ZERO TRUST ЧЕРЕЗ ИЗОЛЯЦИЮ РАБОЧЕЙ СРЕДЫ НА КОНЕЧНОМ УСТРОЙСТВЕ

Для реализации ZTNA-архитектуры обычно используются различные решения. Для проверки личности — различные решения по идентификации и аутентификации пользователей, для проверки устройств и управления доступом — системы управления корпоративными устройствами и учётными записями. Все эти решения требуют разработки политик безопасности и архитектуры, соответствующих концепции «нулевого доверия».

Но что, если совместить всё это в одном решении? Платформа Xello Datacube позволяет реализовать подход Zero Trust, создавая изолированную защищённую среду для работы с корпоративной информацией на устройствах сотрудников. Эта среда разделяет операционную систему на рабочее и личное пространство. Все данные, полученные и созданные внутри защищённого рабочего пространства, остаются в нём в зашифрованном виде без возможности несанкционированного извлечения или кражи.

В отличие от виртуализации, которая требует дополнительных серверных мощностей, изоляция на уровне операционной системы не требует дополнительных ресурсов.

Весь доступ строго регламентирован: сотрудник работает только с теми ресурсами, которые ему разрешены, а все соединения внутри зашифрованы. Работа в рабочем пространстве с данными и ресурсами возможна только через одобренные приложения, которые выдаются прямо из веб-интерфейса Xello Datacube. Это упрощает контроль со стороны ИБ-отдела и снижает нагрузку на инфраструктуру — особенно в больших распределённых командах.

В 2024 году в России утекло более 1,5 млрд записей с персональными данными — на треть больше, чем годом ранее. С 30 мая 2025 года за подобные утечки компаниям грозят штрафы до 15 млн рублей, а при повторных нарушениях — до 3% от годовой выручки.

Zero Trust в платформенном исполнении становится ответом на эти вызовы: он объединяет все ключевые компоненты защиты в единую систему, отслеживает поведение пользователей, жёстко регулирует доступ и позволяет оперативно обновлять политики при изменении уровня риска.

ЗАКЛЮЧЕНИЕ

Пентесты, проведённые компанией Positive Technologies в 2023 году, подтверждают[4]: классических средств защиты недостаточно для борьбы с современными угрозами. В 63% протестированных систем организаций злоумышленник с минимальными знаниями смог проникнуть в локальную сеть. А в 64% случаев был получен доступ к критически важной информации — от интеллектуальной собственности до персональных данных компаний.

Внутренние пентесты выявили[5] ещё более тревожную картину: во многих компаниях злоумышленнику достаточно базовых технических навыков и доступа к открытым эксплойтам, чтобы получить полный контроль над ИТ-инфраструктурой. Это означает доступ ко всем системам, учётным записям, данным и возможностям: от кражи коммерческой информации до остановки бизнес-процессов и вымогательства.

Zero Trust — это про зрелость, осознанность и понимание рисков. В мире, где работа не привязана к офису, а ИТ-среда живёт в облаках, периметра больше не существует. Оставаться в старой логике — значит осознанно выбирать уязвимость.

[4] https://ptsecurity.com/ru-ru/about/news/itogi-pentestov-ot-positive-technologies-96-organizaczij-uyazvimy-pered-kibermoshennikami

[5] https://ptsecurity.com/ru-ru/about/news/itogi-pentestov-ot-positive-technologies-96-organizaczij-uyazvimy-pered-kibermoshennikami