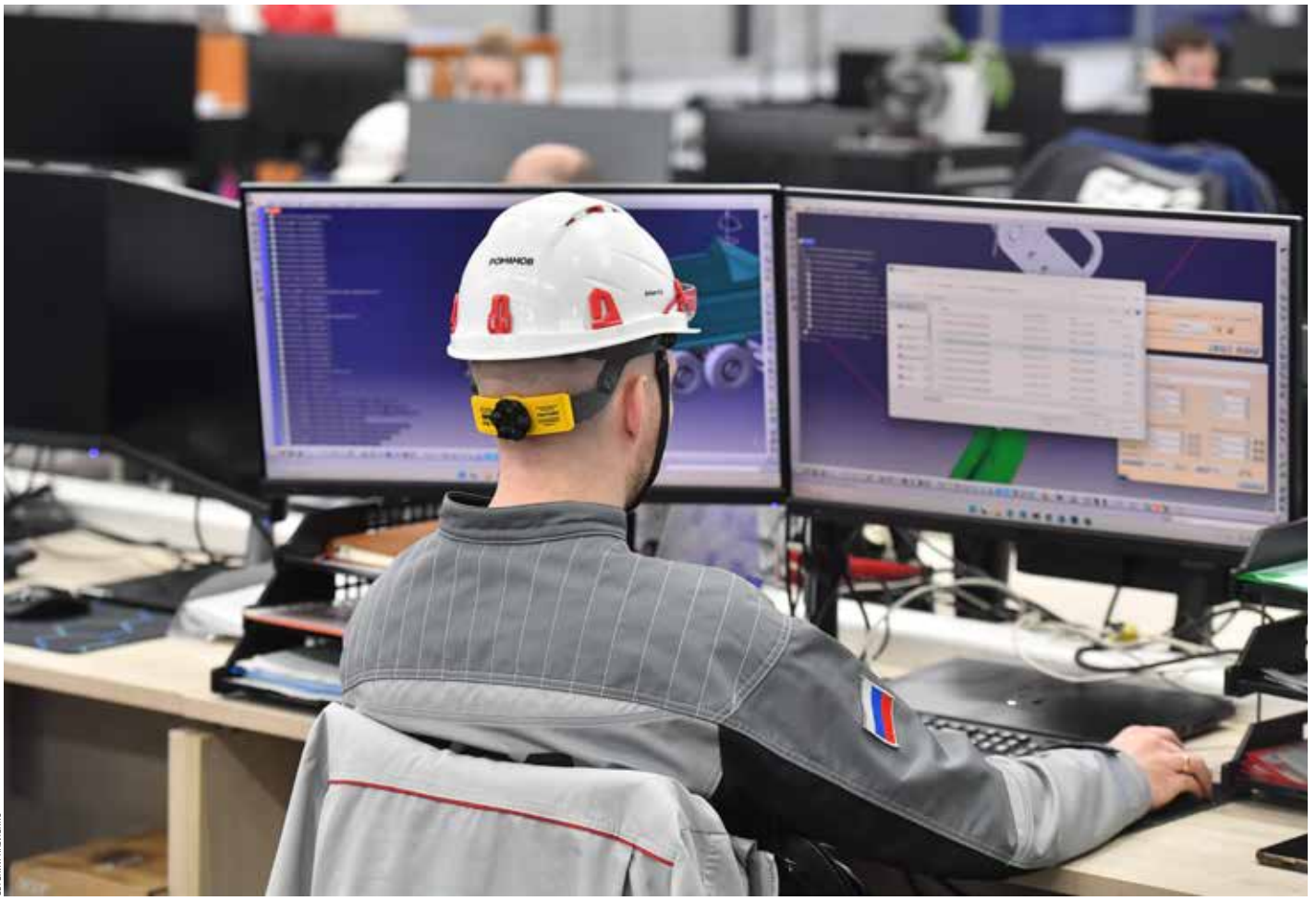
НОЛЬ ДОВЕРИЯ

РОСТ ЧИСЛА КИБЕРАТАК И ВРЕДОНОСНЫХ ВНЕДРЕНИЙ ЧЕРЕЗ ПОДРЯДЧИКОВ ЗАСТАВЛЯЕТ ПРОМЫШЛЕННИКОВ ПЕРЕСМАТРИВАТЬ ПЕРИМЕТРОВУЮ МОДЕЛЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. АРХИТЕКТУРА ZERO TRUST ПРЕДПОЛАГАЕТ ПРОВЕРКУ КАЖДОГО ПОЛЬЗОВАТЕЛЯ, УСТРОЙСТВА И ПРИЛОЖЕНИЯ, А ТАКЖЕ РАЗДЕЛЕНИЕ ИНФРАСТРУКТУРЫ НА ИЗОЛИРОВАННЫЕ СЕГМЕНТЫ. ТАКОЙ ПОДХОД ОГРАНИЧИВАЕТ РАСПРОСТРАНЕНИЕ АТАКИ, ОДНАКО ЕГО ВНЕДРЕНИЕ НА ПРОИЗВОДСТВЕ ТРЕБУЕТ УЧЕТА НЕПРЕРЫВНОСТИ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ И ОБХОДИТСЯ НЕДЕШЕВО. ВИКТОР ИРИСОВ

По данным ИБ-компании «Бастион», около 94% проведенных ею внутренних тестов на проникновение завершилось полным захватом корпоративной сети. Аналитики изучили защищенность более 300 компаний из разных отраслей. Годом ранее доля успешных проникновений составляла 85,7%. Общее количество кибератак за год выросло на 25%, утверждают в «Бастионе». На партнеров и подрядчиков с менее защищенной инфраструктурой пришлось 26% успешных атак. По оценке RED Security, с атаками через подрядчиков была связана треть расследованных инцидентов компрометации инфраструктуры российских компаний, тогда как годом ранее их доля не превышала 10%.



ЕВГЕНИЙ ПАВЛЕНКО

ЭКСПЕРТЫ ОТМЕЧАЮТ, ЧТО ПРИ НЕДОСТАТОЧНОЙ ЗРЕЛОСТИ ПРОЦЕССОВ ОШИБОЧНАЯ РЕАЛИЗАЦИЯ ZERO TRUST МОЖЕТ ПОВЫСИТЬ УЯЗВИМОСТЬ ИНФРАСТРУКТУРЫ

ПОТЕНЦИАЛЬНАЯ КОМПРОМЕТАЦИЯ

Zero Trust, или модель нулевого доверия, исходит из того, что любые пользователи, устройства или приложения по умолчанию считаются потенциально скомпрометированными. Доверие не предоставляется на основании нахождения внутри корпоративного периметра: каждый запрос требует идентификации и проверки, а доступ ограничивается минимально необходимым набором ресурсов.

На место классического сетевого периметра приходит микросегментация, а в основе подхода находится идентификация: каждый запрос автоматически проверяется, а пользователю предоставляются минимально необходимые права доступа только к отдельным разрешенным ресурсам, объясняет руководитель направления продуктовой безопасности Selectel Антон Ведерников. По его словам, эта модель особенно актуальна для облачной и распределенной инфраструктуры, с которой одновременно работают сотрудники и внешние подрядчики.

Микросегментация предполагает разделение сети на отдельные зоны с собственными политиками доступа. Если злоумышленник получает контроль над одним устройством или сервисом, его возможности ограничиваются настройками этого компонента. Это препятствует горизонтальному перемещению внутри сети, повышению привилегий и последующей компрометации критически важных систем.

Ведущий специалист отдела продвижения продуктов «Кода Безопасности» Дмитрий Лебедев сравнивает микросегменты с отсеками океанского судна, где при пробоине в одном из отсеков, то есть при компрометации одного сегмента, закрывается переборка, соединяющая его с другими отсеками-сегментами. Таким образом, злоумышленники получают доступ к ограниченному количеству данных и не могут серьезным образом повлиять на всю инфраструктуру.

Для промышленных предприятий Zero Trust имеет дополнительное значение из-за соседства корпоративной ИТ-инфраструктуры и технологических сетей, управляющих оборудованием. Компрометация офисного сегмента сама по себе не должна давать злоумышленнику возможность перейти к системам промышленной автоматизации.

Вместе с тем механическое применение корпоративных политик безопасности в технологической среде может создавать операционные риски. При внедрении Zero Trust необходимо учитывать требования к непрерывной работе оборудования, недопустимость незапланированных простоев, ограниченные возможности обновления устаревших систем и необходимость удаленного доступа производителей и сервисных подрядчиков.

Если злоумышленнику удается получить доступ к одному из компонентов системы, его возможности ограничены правами и сетевыми настройками этого компонента, говорит господин Ведерников. При этом компании должны заранее определить, каким специалистам и на какой срок необходим доступ к конкретным производственным системам, а также предусмотреть порядок действий при отказе средств идентификации.

ЧЕЛОВЕЧЕСКИЙ ФАКТОР

Эффективность Zero Trust зависит не только от набора технических решений. До начала проекта необходимо инвентаризировать инфраструктуру, описать бизнес-процессы и потоков данных, распределение зон ответственности и разработка политик доступа. После внедрить постоянный мониторинг, пересмотр прав, поиск уязвимостей и проведение киберучений.

По оценке господина Лебедева, при недостаточной зрелости процессов ошибочная реализация модели может, напротив, повысить уязвимость инфраструктуры. Например, концентрация расширенных прав у одного-двух сотрудников формирует новую критическую точку отказа.

Техническая сегментация не устраняет риски, связанные с действиями сотрудников. По данным «Бастиона», только 1% работников сообщает службе безопасности о подозрительных письмах, тогда как 16% переходят по вредоносным ссылкам.

Одновременно снижается стоимость первоначального доступа к корпоративным сетям. Как утверждают в «Бастионе», на теневом рынке такой доступ может стоить $10–50. Криминальная инфраструктура эволюционирует от отдельных сервисных моделей, включая программы-вымогатели и фишинг как услугу, к Crime-as-a-Service — комплексному предложению инструментов для проведения атак.

На этом фоне проверка только при входе в сеть оказывается недостаточной. Zero Trust предусматривает повторную оценку пользователя и устройства на разных этапах работы. Во внимание могут приниматься география подключения, характеристики устройства и нетипичное поведение учетной записи. При обнаружении аномалий доступ блокируется либо требует дополнительного подтверждения.

ИИ В КОНТУР

Распространение корпоративных систем генеративного искусственного интеллекта расширяет область применения Zero Trust. Языковые модели и ИИ-агенты получают доступ к документам, базам данных и внутренним сервисам, фактически превращаясь в самостоятельный тип учетной записи.

К ним принципы Zero Trust применимы буквально, отмечает технический директор направления GenAI Just AI Антон Сипачев. При использовании внешних облачных моделей между сотрудником и сервисом, по его словам, необходим шлюз, способный выявлять и маскировать персональные и конфиденциальные данные.

Для моделей, развернутых внутри корпоративного контура, возникает другая задача. Система, подключенная к внутренней базе знаний, должна наследовать права конкретного пользователя: сотрудник не должен получать через чат-бот документы, недоступные ему напрямую.

Дополнительным риском становится prompt injection — внедрение скрытой вредоносной инструкции в документ, письмо или другой источник, который обрабатывает ИИ. Получив такую команду, агент с избыточными полномочиями может обратиться к закрытым данным или выполнить нежелательное действие. Поэтому его права необходимо ограничивать, а запросы, ответы и обращения к сервисам нужно регистрировать и проверять, полагает господин Сипачев.

К преимуществам Zero Trust участники рынка относят сокращение поверхности атаки, ограничение последствий компрометации и повышение прозрачности инфраструктуры для ИТ- и ИБ-подразделений.

Основными препятствиями остаются стоимость и сложность внедрения. Компаниям приходится пересматривать сетевую архитектуру, модели управления доступом, порядок взаимодействия с подрядчиками и процедуры эксплуатации производственного оборудования. ■