White Paper

Кибербезопасность в ритейле и e-commerce

Содержание

Введение

Интернет изменил способ покупки и продажи товаров и услуг. Сектор розничной торговли и e-commerce продолжают стремительно трансформироваться, а инвестиции в технологии и инновации являются новой ценой ведения бизнеса.

Ожидания потребителей постоянно растут. Они требуют высококачественных продуктов и услуг как на компьютере, так и на мобильных устройствах. В то же время в бэк-энд внедряется аналитика для клиентов и расширенная интеграция с третьими сторонами, что способствует повышению маржи и увеличению доходов. Цифровые платежные системы также обновляются, особенно с появлением небанковских игроков в индустрии платежей, что еще больше поддерживает рост отраслей. Но за эти инновации приходится платить: увеличивается поверхность возможных атак киберпреступников и подверженность ИТ-систем все более изощренным угрозам.

Очевидно, что успешная атака может оказать огромное влияние на бизнес - будь то прямые убытки от нарушения работы компании, отток клиентов из-за удара по репутации, штрафы со стороны регулирующих органов или, скорее всего, сочетание этих трех факторов.

К сожалению, в спешке цифровой трансформации ритейл и компании электронной коммерции часто не успевают за изменениями, когда речь заходит об их кибербезопасности. Киберпреступники, нацеленные на этот сектор, разработали передовые и часто автоматизированные ТТП (тактики, методы и процедуры) для компрометации и монетизации украденных данных. От убедительных фишинговых кампаний, заставляющих пользователей делиться личной и финансовой информацией, до взлома учетных записей с целью совершения мошенничества, целевых вредоносных программ, атакующих PoS, цифровые платежные системы и базы данных клиентов – риски для отрасли еще никогда не были так высоки.

В данном буклете рассматриваются вопросы, с которыми сталкиваются руководители высшего звена в секторе розничной торговли и электронной коммерции, предлагаются идеи и рекомендации по решению проблем.

В современном ландшафте кибербезопасности базовые методы предотвращения угроз информационной безопасности уже не работают. Не проходит и недели без очередного громкого взлома и его финансовых последствий, о которых сообщают СМИ. Но почему ритейлеры все еще подвергаются взломам, несмотря на объем инвестиций в продукты безопасности? Даже самые крупные розничные компании остаются уязвимыми, несмотря на наличие передовых решений SIEM и защиты конечных точек.

Мы рассмотрим вопрос почему розничные компании всех размеров должны предпринимать проактивные шаги для управления своими киберрисками.

Почему ритейл и e-commerce становятся целью хакеров?

В последние годы увеличилось число атак, направленных именно на розничную торговлю. Последствия для бизнеса очевидны: снижение прибыли и падение стоимости бизнеса; негативная реклама, ведущая к снижению доверия потребителей; расходы на ликвидацию последствий взлома и связанные с этим штрафы.

Компании электронной коммерции, которые живут и умирают благодаря онлайн-платежам, подвергаются еще большему риску. Этот сектор особенно уязвим для мошенничества, например, через кражу учетных данных, что приводит к взлому счетов, фроду и связанным с этим расходам на устранение последствий.

Независимо от размера розничной компании или компании электронной коммерции, киберпреступники рассматривают отрасль в целом как главную цель для кибератак из-за данных, которыми располагают эти компании. Чем больше данных вы храните, тем больше цель.

PII потребителей неразрывно связана с платежными данными или данными о держателях карт, необходимыми для совершения транзакций или хранящимися для последующего целевого маркетинга. Уязвимости в программном обеспечении или базы данных клиентов, не использующие достаточный уровень шифрования, становятся целями атаки.

Злоумышленник использует любую из этих уязвимостей и может получить платежную информацию клиентов, что скажется на прибыли компании в виде штрафных санкций за несоответствие требованиям законодательства, а также приведет к репутационному ущербу.

В самой компании скомпрометированные учетные данные сотрудников могут привести к взлому учетных записей, краже личных данных, шантажу, распространению вредоносного ПО, мошенничеству и другим видам преступной деятельности. Изощренные фишинговые кампании, направленные на высокопоставленных лиц и сотрудников могут привести к хаосу в организациях, в то время как целевые вредоносные программы, направленные против ИТ-инфраструктуры могут нарушить работу систем.

Потенциальная финансовая выгода для киберпреступников, стремящихся атаковать сектор розничной торговли и электронной коммерции, огромна. Соответственно, способы, с помощью которых они могут заполучить в свои руки ценные данные, постоянно расширяются. Существует несколько областей, на которые следует обратить внимание компаниям.

Снижение барьеров для покупки

Любая компания в этих отраслях должна внедрять инновации, чтобы оставаться конкурентоспособной. Однако с расширением цифрового присутствия расширяется и поверхность атаки. Многие компании отдают предпочтение быстрым инновациям, направленным на получение прибыли, а не мерам безопасности. Кроме того, постоянное и постепенное совершенствование унаследованных систем может привести к “техническому долгу”. Проще говоря, обеспечение клиентского опыта, позволяющего увеличивать и ускорять покупки, считается более важным, чем поддержание надежных процессов безопасности. В результате эти инновации в сочетании с большими ресурсами, задействованными злоумышленниками, делают сектор розничной торговли весьма привлекательной целью для киберпреступников.

Потребительская аналитика

Успешные компании розничной торговли и e-commerce используют технологии, основанные на данных, используя максимум информации о потребителях, которую они могут законно получить в свои руки, чтобы помочь увеличить продажи и повысить эффективность. Однако эти данные ценны не только для компании, но и для злоумышленников. Чем больше данных, тем привлекательнее цель. После утечки данных они могут появиться на форумах или в дарквебе для продажи. В свою очередь, это может способствовать распространению дальнейших атак, поскольку злоумышленники могут сопоставить эти данные с другими дампами и составить более четкое представление о жертвах.

Платежные системы

Платежные технологии, как традиционные, так и новые, предоставляют злоумышленникам ряд возможностей. Например, на PoS-устройства удивительно легко установить вредоносное ПО, которое записывает данные о каждой карте, используемой в аппарате. Существуют также виды вредоносного ПО, которые могут создавать бэкдоры в других системах организации, сохраняться и распространяться по всей сети, заражая миллионы PoS-устройств и собирая огромные объемы данных.

Между тем, основной сдвиг в способах осуществления платежей сигнализирует отношение потребителей к мобильным кошелькам и NFC, темпы роста которого до 2022 года составят 32%. И эта цифра использует данные только западных рынков; в Китае, например, оплата наличными или картой становится все более редким явлением. Более того, многие компании стремятся включить технологию автоматических платежей в свои приложения, но сопутствующие защитные меры еще не доведены до совершенства.

Совершенно очевидно, что распространение онлайн-рынков означает, что бренды становятся все более уязвимыми. Не в последнюю очередь это связано с тем, что мошенники предпочитают цифровые транзакции, позволяющие обойти технологию чипов и пинов.

Управление данными

Многие ритейлеры склонны применять подход к сбору и хранению данных, основанный на соблюдении требований законодательства. Хотя это оправдано перед лицом жесткого законодательства, включая 152-ФЗ и GDPR, часто это происходит в ущерб надежной системе управления данными в целом. Например, часто существует зависимость от сторонних поставщиков (в сфере обслуживания клиентов и т.д.), что приводит к пробелам в структурах контроля, которыми могут воспользоваться злоумышленники. Кроме того, сегодня, как никогда ранее, успешная атака может привести к тому, что первоначальный сборщик данных - розничная компания - будет наказан. Стоит помнить, что компрометация только одного поставщика открывает злоумышленникам возмодности для атак на новые цели.

Человеческий фактор

Как и все отрасли, розничная торговля и e-commerce не застрахованы от атак с помощью социальной инженерии. Фишинговые кампании в этих секторах особенно успешны, что обусловлено, с одной стороны, низким уровнем осведомленности сотрудников в области кибербезопасности, а с другой - широким влиянием бренда.

Сценарий, при котором сотрудники стали жертвами фишинговой кампании, содержащей вредоносное ПО , может скомпрометировать учетные данные для входа в систему, а затем и внутренние сервисы и системы компании.

Даже если атака затронула всего несколько сотрудников, достаточно одной скомпрометированной учетной записи, чтобы злоумышленники получили возможность попасть в инфраструктуру и сохраняться там, нанося ущерб, когда обнаружится что-то очень ценное. К моменту обнаружения нарушения, как правило, уже слишком поздно.

С другой стороны, огромное количество электронных писем (маркетинговые, , информацию об отправке и т.д.) делает выявление попытки мошенничества среди законного контента еще более сложной задачей.

Количество доменов, которыми владеют розничные компании, особенно те, которые работают на нескольких рынках, также означает, что компании и их клиенты могут стать жертвами кибersквоттинга, поскольку существует больше доменов, которые можно использовать.

В целом, сектор розничной торговли и электронной коммерции очень уязвим для атак по ряду причин, некоторые из которых уникальны для этой отрасли, а другие распространены во всех секторах. В следующем разделе будет рассмотрено состояние отрасли, включая изучение ландшафта угроз.

Состояние отрасли

Как уже говорилось выше, компании розничного сектора и e-commerce являются весьма привлекательными целями для злоумышленников и киберпреступных организаций.

По мере цифровой трансформации число векторов атак, доступных киберпреступникам, расширяется и угрожает компаниям любого размера. Нарушение данных о потребителях представляет собой огромный бизнес-риск для компаний, но на каждую успешную атаку, в ходе которой похищаются данные кредитных карт или PII, приходится ряд других угроз, от которых компаниям необходимо защищаться.

Например, DDoS-атаки, выводящие из строя сайты магазинов в праздничный сезон, или поддельные сайты, выдающие себя за настоящие. В прошлом году атаки вредоносных программ, похищающих данные через сайты электронной коммерции, были особенно активны в России и на других развивающихся рынках.

Киберугрозы

В этом разделе будут описаны некоторые из наиболее активных киберугроз, с которыми сталкивается розничная торговля. Командам, отвечающим за безопасность, будет полезно обратить внимание на график их устойчивости к различным категориям угроз.

Категория	Злоумышленник	ТТП
Базовая	Низкоуровневый	Известные уязвимости и инструменты.
Продвинутая	Изощренный; APT, хакерские групировки	Целевое ВПО; сложные инструменты и методы, угрозы нулевого дня
Новая	Изощренный; APT, хакерские групировки, государства	Выявления эксплойтов; новые векторы атак

Фишинг

Фишинг - это основная техника, используемая киберпреступниками для кражи учетных данных и персональных данных у своих жертв. Он остается одним из наиболее эффективных векторов атак, поскольку обычно используется вместе с методами социальной инженерии для получения информации от своих жертв. Отправитель пытается заставить жертву перейти по ссылке и ввести учетные данные, персональную информацию или установить вредоносное ПО. Когда фишинг направлен против отдельного человека или компании, он известен как spear phishing.

Успех атаки часто зависит от уровня социальной инженерии и качества коммуникации. Часто злоумышленники используют логотипы компаний и реалистично выглядящие ссылки, чтобы обмануть ничего не подозревающих клиентов.

Фишинг может быть использован для распространения вредоносного ПО для точек продаж (POS), часто в сочетании с удивительно смелыми методами социальной инженерии, например, звонками жертвам, чтобы убедить их открыть вредоносные файлы.

Вызывает беспокойство тот факт, что в секторе розничной торговли количество попыток фишинга в прошлом году увеличилось на 78%.

Поддельные сайты

Поддельные веб-сайты представляют реальную опасность для розничных компаний. Важность онлайн-покупок во всем секторе означает, что большие инвестиции в обслуживание клиентов открывают новые возможности для киберпреступников. Чем шире предложение, тем выше риск, поскольку компания обязательно будет иметь большее количество URL-адресов, которые можно сымитировать. Если, например, у розничной компании есть несколько различных.

Тщательно созданный поддельный сайт перенимает дизайн целевого сайта, логотипы, шрифты и часто имеет похожий URL-адрес - или такой, который выглядит достаточно легитимным, чтобы убедить посетителя в безопасности сайта. Поддельный сайт может использоваться для различных целей, включая продвинутые фишинговые кампании, распространение вредоносных программ и сбор информации о посетителях, которая впоследствии может быть использована в преступных целях. Важно повышать устойчивость к внешним и внутренним угрозам, находя и исследуя фейковые сайты.

Мошенничество при возврате денег

Мошенники заинтересованы в получение возврата денег за товары от крупных розничных продавцов под ложным предлогом. Как и фишинг, мошенничество с возвратом денег не использует скомпрометированную информацию о платежных картах, а полагается на методы социальной инженерии для обеспечения возврата денег. Мошенники, занимающиеся мошенничеством с возвратом денег, пытаются заставить представителей службы поддержки поверить, что при отправке или доставке покупки возникли проблемы. Распространенные выдумки, которые используют злоумышленники, надеющиеся добиться возврата денег, заключаются в том, что посылка не пришла, посылка была украдена, посылка была пустой или что предметы в посылке были каким-то образом испорчены.

Вредоносное ПО

Вредоносные программы широко используются киберпреступниками для получения конфиденциальной информации. Атака может представлять собой длительную компрометацию данных и метаданных о торговых точках и транзакциях по кредитным картам, которые попали к злоумышленникам. Возможная родолжительность таких атак свидетельствует о необходимости инвестировать в надлежащие системы предотвращения и обнаружения, чтобы избежать или обнаружить вторжения в сеть компании.

Банковские трояны

Банковские трояны - это тип вредоносного ПО, специально разработанный для получения банковских и платежных данных от своих жертв. Еще 2018 году “Лаборатория Касперского” определила основные семейства вредоносных программ, использующих бренды электронной коммерции для кражи. Все они являются банковскими троянами, наиболее известными тем, что нацелены на пользователей финансовых онлайн-сервисов для получения банковских и платежных данных.

Трояны обладают множеством функций, позволяющих им похищать у жертвы информаци. Например, регистрация нажатий клавиш и захват форм. Веб-инъекция - это техника, используемая для перехвата данных после их расшифровки по протоколу SSL, но до их отображения в браузере. Таким образом, троян получает возможность изменять ответ сервера веб-страницы. Этот ответ используется троянами для запроса дополнительной информации у жертвы, в том числе для совершения мошеннических операций.

Основными объектами атак этого типа являются организации в секторе финансовых услуг, но в последние годы очевидно, что цель сместилась в сторону розничной торговли. Злоумышленники совершают эти атаки, пытаясь завладеть учетными данными пользователей через поддельные панели входа и совершить мошеннические действия от имени пользователей.

Такое ПО в основном распространяются через почтовые спам-кампании и наборы эксплойтов, которые обычно используют загрузчик для инсталяции фактического трояна. Также, известно, что киберпреступники используют бэкдоры для установки пользовательских вредоносных программ и перемещения по сети с целью добычи конфиденциальных данных. Анализ угроз имеет решающее значение не только для поиска вне сети, но и для обнаружения того, что уже находится внутри ИТ-инфраструктуры.

Вирусы-вымогатели

Цель вирусов-вымогателей - проникнуть в инфраструктуру компании и взять ее под контроль. Когда вредоносная программа успешно заражает машину, она шифрует все важные файлы и данные.

Ransomware-as-a-Service - это бизнес-модель, при которой программное обеспечение вируса-вымогателя может быть предоставлено в аренду любому клиенту, готовому заплатить соответствующую цену. Разработчики вредоносного ПО предлагают его третьим лицам по доступной цене или получая процент от выручки. Некоторые RaaS даже имеют собственные команды поддержки клиентов, которые помогают использовать программное обеспечение, решая возникающие проблемы. Такая модель киберпреступного бизнеса является беспроигрышной для разработчиков вредоносных программ: они создают мощное, но простое в использовании программное обеспечение, которое могут использовать другие лица.

Такая бизнес-стратегия делает RaaS особенно опасной угрозой из-за неопределенной клиентской базы. От обычных пользователей до компаний, заинтересованных в нарушении деятельности своих конкурентов, - любой человек может стать потенциальным субъектом угрозы.

Часто разработчики RaaS пытаются сделать свои продукты привлекательными для неквалифицированных пользователей, создавая интуитивно понятные онлайн-порталы управления для развертывания и отслеживания арендованного ransomware. Они даже позволяют клиентам настраивать некоторые параметры, такие как цена выкупа или сообщение, показываемое жертвам.

Мобильные приложения

В последние годы использование смартфонов для покупки товаров увеличилось в геометрической прогрессии, соответственно, увеличилось и количество вредоносных программ, разработанных для этой цели.

Похищение учетных записей и мошеннические транзакции стали широко распространены, и только недавно приложения для розничной торговли стали использовать методы аутентификации во время обмена данными между приложением и серверами для подтверждения.

Вредоносное ПО для POS

Несмотря на то, что это одна из самых простых форм кибератак, вредоносные программы для PoS, предназначенные для кражи реквизитов карт очень эффективны. Сочетание труднообнаруживаемых вредоносных программ, проникающих в устаревшее оборудование, которое трудно патчить, и общих уязвимостей ОС означает, что эта конкретная угроза распространена и от нее трудно защититься.

Цифровой скимминг

Цифровые скиммеры - это скрипты, предназначенные для кражи данных, вводимых в формы онлайн-платежей, которые злоумышленники используют на взломанных веб-сайтах организаций электронной коммерции или сторонних поставщиков.

Исследования показывают, что для облегчения совершения преступлений злоумышленники часто используют уязвимости в веб-сайте/CMS или захватывают учетные записи хостинга/CMS.

DDoS-атаки

Компании, которые в значительной степени полагаются на онлайн-продажи, особенно подвержены распределенным атакам типа “отказ в обслуживании”, или DDoS-атакам.

Атаки направлены на пропускную способность сайтов электронной коммерции и призваны нарушить работу бизнеса, нанеся серьезный ущерб трафику и базам данных. В результате вовремя проведенной атаки, например, в период оживленных покупок, компания может понести огромные убытки.

Даже небольшая атака, перегружающая серверы и выводящая сайт из строя на несколько секунд, может расстроить клиентов настолько, что они начнут совершать покупки в других местах. Кроме того, злоумышленники могут попытаться вымогать деньги у ритейлера, просто угрожая DDoS-атакой. К потерям от DDoS-атаки следует добавить и расходы на устранение последствий.

Уязвимости третьих сторон

Хотя компании должны вкладывать значительные средства в собственную инфраструктуру кибербезопасности, сторонние поставщики могут стать слабым звеном в системе обеспечения безопасности.

Новые платежные технологии внедряются как розничными компаниями, так и другими предприятиями, но они создают дополнительные риски. По данным Deloitte, лишь немногие потребительские компании регулярно проверяют и тестируют возможности своих поставщиков в области кибербезопасности.Утечки данных часто начинаются с компрометации поставщиков и подрядчиков.

Существуют значительные трудности с наймом и обучением ИТ-специалистов, поэтому привлечение поставщиков для разработки бэк-энда (например, для облачных интеграций, разработки приложений, мобильных платежей) может привести к тому, что ритейлеры окажутся под угрозой новых вызовов кибербезопасности.

Хактивизм

Хотя компании всех размеров конкурируют друг с другом на рынке, хактивисты не делают такой же дифференциации и могут атаковать любую розничную компанию в результате недовольства конкретной организацией. Если какая-либо крупная компания вовлечена в спорную ситуацию, эффект от этого может быть значительным для всего сектора. Если хактивистам не удается проникнуть в одну компанию, им может больше повезти с конкурентом. Тем самым, привлекая внимание к слабым сторонам сектора в целом, и нанося при этом значительный репутационный ущерб.

Управление рисками кибербезопасности

Проще говоря, невозможно защитить все данные, сети и приложения. Организации должны внедрять проактивные меры безопасности, которые помогут им определить приоритеты в обнаружении и реагировании, что позволит им быстро реагировать на инциденты. В этом разделе рассматривается ряд стратегий и механизмов, которые могут внедрить розничные компании любого размера.

Взаимодействие на уровне руководства

Прежде всего, руководство компании должно быть полностью вовлечено в процесс кибербезопасности. Защита предприятия от постоянно меняющегося динамического ландшафта угроз больше не является прерогативой ИТ-директора, CISO или ИТ-команды. Кибербезопасность - это работа каждого, и руководство компании несет ответственность за создание и поощрение вовлечения к снижению киберрисков во всем бизнесе.

Необходимо убедиться, что сотрудники, прямо или косвенно вовлеченные в любые проекты, связанные с риском для бренда, включают оценку безопасности в каждое из действий, проектов и процессов.

В целом, очень важно создать сильную культуру кибербезопасности в организации. Она должна распространяться от руководящего состава вплоть до новых сотрудников, поощряя их к полному пониманию рисков, связанных с использованием определенных технологий.

Частое обучение в масштабах компании приветствуется, и хотя обучение и бербезопасности крайне важно для любого предприятия, независимо от его размера, надежная культура безопасности в крупных компаниях особенно важна просто из-за масштаба технологий и персонала.

Реагирование на нарушения

Репутация имеет решающее значение для компаний отрасли. Негативное восприятие бренда может оказать существенное влияние на итоговые показатели. В связи с этим, приоритетом должно стать обеспечение высокого уровня готовности к реагированию на нарушение кибербезопасности, чтобы свести к минимуму сбои в работе, которые практически неизбежны.

Розничные компании должны с самого начала продумать план действий, чтобы в кратчайшие сроки добиваться принятия жестких решений по устранению или минимизации ущерба от кибернарушений. Планирование сценариев и тренинги также играют ключевую роль, как и наблюдение за тем, что происходит на рынке - ошибки других компаний не должны стать вашими собственными.

Также полезно исходить из того, что любое нарушение в конечном итоге станет достоянием общественности и его будет трудно скрыть. Поэтому назначение пресс-секретаря и заблаговременная подготовка планов кризисных коммуникаций являются конструктивными мерами. Наконец, подготовка должна включать налаживание взаимодействия с другими командами, которые могут помочь в случае нарушения, как внутри компании, так и за ее пределами. В их число должны входить правоохранительные органы, юридические службы, специалисты по связям с общественностью и поставщики данных об угрозах, которые могут помочь в реагировании на нарушения.

Безопасность платежных систем

Ни одна платежная система не защищена на 100%, и очевидно, что одной из самых главных целей для киберпреступников являются платежные данные. Поэтому как для предприятий, так и для потребителей очень важно, чтобы платежные системы были максимально защищены, и есть ряд шагов, которые могут предпринять ритейлеры.

Многие из них подразумевают постоянный анализ и оценку существующих механизмов. Все платежные технологии (особенно те, которые используют третьи стороны) должны подвергаться строгому и постоянному мониторингу, с регулярным сканированием уязвимостей, чтобы быть в курсе последних исправлений безопасности. Также приветствуются процессы, которые ведут инвентаризацию конечных точек платежей, таких как PoS-устройства.

Безопасность третьих лиц

Компании, которые обязательно передают данные клиентов внешним партнерам, должны добиваться самого высокого уровня безопасности. Зачастую число сторонних поставщиков исчисляется десятками, если не сотнями, в зависимости от размера компании. Чтобы помочь справиться с этим, многоуровневая система безопасности может помочь сегментировать и оценить эти компании в зависимости от уровня риска, который они представляют для бизнеса.

Например, сторонний провайдер платежей может относиться к первому уровню, учитывая обрабатываемую им информацию. Ритейлерам следует с самого начала продумать план действий по реагированию на нарушение третьих лиц. Все платежные технологии (особенно те, которые используют третьи стороны) должны подвергаться строгому и постоянному мониторингу.

Тенденция к децентрализации операционных функций означает, что разработка и внедрение комплексной программы по управлению рисками, связанными с третьими сторонами, имеет решающее значение. Разумно определить требования к сторонним поставщикам на этапе закупок и регулярно контролировать их выполнение. В достижении этой цели могут помочь модули анализа угроз.

Предотвращение мошенничества

Попытки мошенничества со стороны киберпреступников могут увенчаться успехом разными способами. Они не только обманывают покупателей, лишая их личной информации, но и лишают ритейлера товаров, а также могут нанести значительный репутационный ущерб. Когда речь идет, например, о краже учетных данных клиентов, всего одна хорошая учетная запись может открыть дверь в организацию и вызвать хаос. Киберпреступник может выдать себя за реального клиента, чтобы украсть товары или совершить мошеннические операции - и в большинстве случаев именно ритейлеру придется нести расходы.
Такие атаки обычно осуществляются субъектами угроз, которые хотят быстро выиграть на украденных учетных данных. Это не характерно для продвинутых угроз, поскольку они используют эти учетные записи для других целей (повторные поставки, отмывание денег, мошенничество с подарочными картами и т.д.: подробнее см. наш отчет об экосистеме кражи учетных данных). Однако подобные атаки обходятся розничным торговцам и компаниям электронной коммерции в значительную сумму денег, которая растет с каждым годом.
Чем быстрее организации обнаружат эти скомпрометированные учетные данные, тем лучше. При использовании модулей анализа угроз, если они будут обнаружены в течение нескольких дней после компрометации (а не обычных месяцев), то последствия атаки могут быть значительно снижены.

Корпоративное обучение

Обучение кибербезопасности может снизить риск для розничных компаний. Обучение должно быть направлено не только на внутреннюю безопасность, но и на то, как сотрудники управляют своей личной информацией, BYOD, учетными данными в целом - постоянная бдительность при любом сценарии является ключом к минимизации риска в масштабах компании.

Многие розничные компании не обучают своих сотрудников должным образом. Это может быть связано с затратами, высокой текучестью кадров или просто нехваткой ресурсов. Однакопредоставление возможностей для регулярного обучения должно способствовать формированию культуры кибергигиены в организации.

На более оперативном уровне регулярные внутренние фишинговые тесты, помогающие сотрудникам лучше определять потенциальные угрозы, в сочетании с имитацией реальных сценариев угроз также являются полезными шагами. Оценивая результаты этих тестов, розничные компании могут выявить пробелы и потенциальные уязвимости (в том числе среди персонала) и постараться устранить их, пока не стало слишком поздно.

Заключение

В данном документе мы постарались осветить проблемы, с которыми сталкиваются розничные компании. Сохранение конкурентоспособности на современном рынке означает, что новые технологические инициативы внедряются в сжатые сроки и в рамках ограниченных бюджетов, а кибербезопасность не заложена с самого начала, как это должно быть.

В розничной торговле, в частности, все хранящиеся данные должны рассматриваться как стратегический актив компании, от информации о клиентах до IP-адресов. При этом ритейлеры понимают, что это делает данные чрезвычайно ценной целью для киберпреступников, которые представляют огромный риск для бизнеса в случае атаки или попытки мошенничества.

В конечном итоге все сводится к правильным инвестициям. Розничные компании должны стараться быть на шаг впереди злоумышленников. Инновации внутри компании и сотрудничество с компаниями в сфере ИБ помогают оценить и укрепить киберустойчивость в критически важных областях.

Чем мы можем Вам помочь?

ООО «НТЦ ЕВРААС», являясь многопрофильной коммерческой структурой, имеет все необходимые лицензии регуляторов рынка информационной безопасности, в том числе лицензии на осуществление работ с использованием сведений, составляющих государственную тайну.

Обладая фундаментальными знаниями и опытом в области защиты информации, эксперты НТЦ «ЕВРААС» предлагают новейшие комплексные разработки в сфере обеспечения безопасности компаний розничной торговли.

Мы проектируем системы под конкретные нужды и специфику организаций, тем самым гарантируя, что система информационной безопасности комплексно решает все задачи и обеспечивает надежную круглосуточную защиту ваших корпоративных ресурсов и данных.

Контакты:

г. Москва, ул. Автозаводская 13/1

8 (495) 748-09-44

evraas@evraas.ru