White Paper

Компрометация деловой электронной почты (BEC)

Содержание

Введение

Компрометация деловой электронной почты (BEC) в 2020 году обошлась организациям в более чем 1,7 миллиарда долларов. Одних технологий кибербезопасности недостаточно для борьбы с этой угрозой. Компании могут добиться успеха в противодействии BEC только благодаря сочетанию обучения по вопросам безопасности, технологий защиты электронной почты и изменений в бизнес-процессах.

Компрометация деловой электронной почты (BEC) - это быстро растущая киберугроза, которая уже наносит больший финансовый ущерб, чем любой другой вид киберпреступлений.

Ожидается, что число атак BEC продолжит расти. По данным исследований, шестьдесят процентов организаций отметили рост числа атак по компроментации деловой электронной почты за последний год. По прогнозам Gartner, Inc., ущерб от фишинговых атак BEC будет удваиваться каждый год, превысив в 2023 году 5 миллиардов долларов.

Основные проблемы

- Компрометация деловой электронной почты - основная причина финансовых потерь, связанных с кибербезопасностью;
- Поскольку фишинговые письма не вссегда содержат вредоносные ссылки или вложения, их невозможно обнаружить с помощью традиционных методов сканирования содержимого электронной почты;
- Злоумышленники также могут использовать BEC для обмана клиентов вашей организации или других участников экосистемы вашего бизнеса.

Рекомендации

- Используйте сочетание тренингов по безопасности корпоративной почты с техническими средствами обеспечения безопасности.

- Используйте DMARC для предотвращения подделки домена, защиты вашего бренда и прекращения атак на ваших клиентов и деловых партнеров.

- Эффективные тренинги по повышению осведомленности в области безопасности являются ключом к снижению количества человеческих ошибок, что является фактором всех успешных атак BEC.

- Используйте передовое решение безопасности электронной почты для выявления и предотвращения попыток компрометации деловой электронной почты.

- Внедряйте дополнительные этапы проверки в процессах, связанных с платежами, таких как запросы на электронные переводы или изменение информации о банковском счете.

Компрометация деловой почты (BEC)

Атаки BEC - это фишинговые аферы с использованием электронной почты. Цель BEC - обманом заставить людей совершить платеж или предоставить злоумышленнику конфиденциальную информацию.

Чтобы завоевать доверие пользователей, злоумышленники используют методы социальной инженерии. Они выдают себя за доверенных лиц или организации - например, генерального директора компании или одного из поставщиков - и отправляют фишинговые электронные письма лицам, имеющим полномочия для осуществления платежей. Эти атаки, как правило, невозможно обнаружить с помощью традиционной технологии сканирования электронной почты, поскольку фишинговые письма не содержат вредоносных вложений или вредоносных ссылок.

Атаки BEC различаются по степени сложности. Некоторые атаки тщательно продуманы, что делает их чрезвычайно опасными. Другие - гораздо более примитивны, но все равно часто приводят к успеху.

При наиболее сложных атаках злоумышленники тщательно изучают свои цели в Интернете, исследуя такие источники, как аккаунты в социальных сетях и веб-страницы организации. Это позволяет им определить сотрудников обладающих полномочиями запрашивать и санкционировать платежи, понять взаимоотношения между ними и составить электронные письма, содержащие информацию, необходимую для того, чтобы убедить людей в том, что они получают настоящий платежный запрос.

Типы атак

Большинство атак BEC можно разделить на несколько основных типов, хотя существует множество вариаций.

Имитация действий руководителя

В этом типе атак злоумышленник, выдающий себя за генерального директора, финансового директора или другого руководителя, отправляет запрос на оплату по электронной почте человеку с полномочиями - например, сотруднику, работающему в отделе закупок.
.
Такие атаки часто начинаются с короткого, относительно неформального сообщения, призванного втянуть жертву в разговор по электронной почте. Злоумышленник может создать ощущение срочности, чтобы заставить жертву ответить, не тратя время на проверку легитимности сообщения. Например: “Я нахожусь на встрече и мне срочна нужна помощь, не могли бы вы быстро помочь мне кое с чем?”.

Заинтересовав жертву, злоумышленник переводит разговор на просьбу о платеже. Такие атаки BEC часто особенно убедительны, поскольку они используют существующие отношения и роли в организации.

Проводя разведку в Интернете, злоумышленник уже знает, что жертва подчиняется финансовому директору, поэтому в своем запросе по электронной почте он выдает себя за финансового директора.

Злоумышленники находят личную информацию о финансовом директоре или своей жертве на корпоративном сайте или в социальных сетях, поэтому они могут включать в сообщение определенные детали, чтобы письмо выглядело более достоверным. Жертва привыкла получать и исполнять платежные запросы от финансового директора. BEC-атака выглядит как обычный запрос, который является частью повседневной деятельности, и, как следствие, она с большей вероятностью будет успешной.

Имитация действий поставщика

Злоумышленники выдают себя за поставщиков организации, используя электронные письма, содержащие поддельные счета-фактуры или информацию о изменениях в банковских реквизитах. Как и в случае с имитацией действий руководителя, эти атаки часто используют существующие отношения, чтобы выглядеть более убедительно.

Например, злоумышленники могут установить использовать фейковые домены или создать веб-страницы, похожие на сайты реальных поставщиков, а также подделать счета-фактуры и другие документы.

Мошенничество с зарплатой

Эти атаки обычно направлены на сотрудников отдела кадров и финансовых подразделений. Обычно они выглядят как просьбы сотрудника изменить реквизиты его банковского счета для прямого перечисления зарплаты. В действительности денежные средства направляются на счет, контролируемый злоумышленником.

Кража данных

Этот вариант атак направлен на получение личной информации или других конфиденциальных данных. Злоумышленники отправляют электронные письма в кадровые службы или другие отделы, запрашивая личную информацию о сотрудниках. Впоследствии эта информация может быть использована для кражи личных данных, мошенничества или других финансовых махинаций.

Внутренние и внешние атаки

Злоумышленники могут завладеть внутренними учетными записями электронной почты с помощью вредоносных программ или фишинговых писем, предназначенных для кражи учетных данных, а затем использовать учетные записи электронной почты для отправки внутренних запросов сотрудникам организации.

Злоумышленники также могут использовать эти учетные записи электронной почты для атак BEC на клиентов или деловых партнеров организации. Эти атаки особенно трудно обнаружить, поскольку они исходят с легитимных адресов электронной почты.

Обнаружение и предотвращение

Обнаружение и предотвращение атак по компрометации деловой электронной почты представляет собой сложную задачу. Атаки BEC обычно не могут быть обнаружены с помощью традиционной технологии сканирования электронной почты, поскольку фишинговые письма не содержат вредоносных вложений или ссылок.

Вместо этого организации должны использовать сочетание обучения по вопросам безопасности, передовых технологии защиты электронной почты, способных выявлять попытки выдачи себя за другого человека, и более строгих регламентов авторизации платежей и других процессов.

Тренинги по безопасности

Все успешные атаки по компрометации деловой электронной почты включают элемент человеческой ошибки. Обучение по вопросам кибербезопасности может значительно снизить вероятность человеческой ошибки и поэтому играет важную роль в любой стратегии по предотвращению BEC.

Обучение по вопросам безопасности должно знакомить пользователей с конкретными методами, используемыми при фишинговых атаках и попытках BEC. Чтобы обучение было максимально эффективным оно должно проводиться с учетом новейших методов киберпреступников, а также с использованием специализированного программного обеспечения (например, Pfishman).

Обучение должно включать симуляторы фишинга, которые позволят организации объективно оценить осведомленность сотрудников и их способность распознавать атаки. Ключевое сообщение, которое необходимо донести до сотрудников, что электронная почта сама по себе не является адекватной формой аутентификации - она должна быть дополнена другими методами.

Организациям следует выявлять сотрудников, подверженных повышенному риску, и проводить для них дополнительное обучение. Такие сотрудники могут быть определены по их ролям: пользователи, отвечающие за платежи или имеющие привилегированный доступ по другим причинам, могут быть особенно подвержены фишингу. Некоторые решения для защиты электронной почты могут определять, какие внутренние пользователи наиболее часто становятся мишенью фишинговых кампаний. В рамках обучения важно предоставить пользователям четкий механизм для сообщения о попытках BEC.

Организациям также следует рассмотреть возможность распространения обучения на других ключевых членов экосистемы бизнеса, включая клиентов, поставщиков и партнеров.

Безопасность электронной почты

Ни одна технология не может остановить все атаки BEC. Однако передовые системы безопасности электронной почты могут выявить и предотвратить многие попытки BEC. Облачные шлюзы безопасности электронной почты могут работать с корпоративными системами электронной почты, анализируя входящую и исходящую почту для обнаружения и предотвращения угроз. Технологии безопасности должны защищать пользователей на всех используемых ими устройствах, включая настольные, мобильные и персональные устройства.

Фишинговые атаки трудно обнаружить. Злоумышленники могут использовать различные методы, чтобы замаскировать свои атаки под настоящие электронные письма.

Не существует единого индикатора, который можно было бы использовать для надежной идентификации входящего электронного письма, как фишинговой попытки BEC. Поэтому для определения вероятности того, что входящее письмо является попыткой выдачи себя за другого человека, решение для защиты электронной почты должно идентифицировать множество предупреждающих признаков.

При попытке создания убедительных фишинговых писем злоумышленники могут манипулировать лишь ограниченным числом характеристик сообщения. В основном, они используют поддельную информацию об отправителе, создаюи убедительный текст в теле или теме сообщения, а также прикрепляют файлы. Решения для защиты электронной почты может изучить все эти характеристики, чтобы определить легитимность входящей электронной почты. При обнаружении достаточного количества признаков служба отклонит или пометит сообщение.

К типичным предупреждающим признакам относятся:

- Отображаемые имена отправителей, которые не соответствуют реальному домену отправителя и поэтому могут указывать на попытку подмены домена.

- Письма, отправленные с доменных имен, которые похожи на доменное имя вашей организации или на имена известных брендов или доверенных третьих лиц.

- Письма с недавно зарегистрированных доменов, которые указывают на то, что домен мог быть зарегистрирован в злонамеренных целях.

- Ключевые слова в теле сообщения. Все попытки BEC в конечном итоге содержат запрос, как правило, на оплату или получение данных. Чтобы сделать такой запрос, электронное письмо должно содержать определенные словосочетания, например, “банковский перевод”. Решение для защиты электронной почты может искать в тексте сообщения самые разные ключевые слова.

DMARC

DMARC - это стандарт проверки электронной почты, который защищает от подмены домена. Он может помочь вашей организации предотвратить использование злоумышленниками вашего бренда в BEC-атаках на ваших клиентов или другие организации. Он также позволяет провайдерам электронной почты отфильтровывать многие входящие BEC-атаки до того, как они достигнут вашей организации.

Чтобы использовать DMARC для защиты вашего бренда, сначала необходимо определить все домены, связанные с вашей организацией.

Затем вы устанавливаете политики, определяющие, что должны делать почтовые системы, если они получают электронные письма, подделывающие эти домены.

Системы электронной почты проверяют входящие сообщения на соответствие политикам DMARC и определяют, принимать, отклонять или помещать почту в карантин. Большинство основных платформ электронной почты применяют проверку DMARC к получаемым письмам. Ваша организация получает отчеты от этих провайдеров, которые помогают отслеживать и предотвращать попытки эксплуатации бренда.

Поскольку настройка DMARC может быть сложной, а отчеты - трудночитаемыми, рекомендуется использовать коммерческий инструмент для управления и анализа внедрения DMARC.

Изменение процессов

По данным Gartner Inc., изменения в процессах согласования платежей могут помочь в предотвращении BEC-мошенничества. Например, подобно процессу многофакторной аутентификации, организация может предусмотреть, что любые запросы по электронной почте на изменение реквизитов должны проверяться другими методами, например, телефонными звонками.

Заключение

Бороться с быстро растущей угрозой компрометации деловой электронной почты непросто, но возможно. Для предотвращения атак, связанных с компрометацией деловой электронной почты, необходима последовательная стратегия, которая включает в себя обучение по вопросам безопасности, технологии защиты электронной почты и изменения во внутренних процессах. Эффективная стратегия не только поможет защитить вашу организацию от кражи денег и конфиденциальных данных, но и защитить ваших клиентов, деловых партнеров и вашу репутацию.

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