ПРИНЦИПЫ ЦИФРОВОЙ БЕЗОПАСНОСТИ: КАК ЗАЩИТИТЬ СЕБЯ И ЧТО ДЕЛАТЬ В СЛУЧАЕ КРИЗИСА?

НЕСГИБАЕМАЯ ПРИБАЛТИКА

В современной цифровой среде то, что мы делаем в Интернете, является отражением происходящего в реальной жизни. Как и в физическом мире, никто не защищен от мошенничества, кражи, введения в заблуждение и других угроз, возникающих на цифровых платформах. Эволюция цифровых технологий и услуг дала возможность нечестным людям и организациям добывать и использовать данные себе во благо множеством изобретательных методов. Однако меры безопасности реального мира, такие как запирание дверей и установка сигнализации, имеют свои эквиваленты и в Интернете, позволяя выявлять риски и защитить себя от кибератак.

Что такое кибератака?

Кибератака означает преднамеренные попытки киберпреступников, хакеров или других злоумышленников проникнуть в компьютер, телефон или систему. Основными целями кибератаки обычно являются искажение, кража или уничтожение информации. Злоумышленники могут руководствоваться финансовыми, политическими мотивами или даже соображениями конкуренции.

Наиболее популярные виды кибератак:

- ***Вредоносное программное обеспечение.*** Любая программа или код, разработанный специально для причинения вреда компьютеру, сети или серверу. Это – самый распространенный вид кибератак.

- ***Атака на отказ в обслуживании (Denial of Service, DoS).*** Целенаправленное нападение, которое наводняет сеть искусственными запросами, чтобы нарушить работу предприятия. Во время DoS-атаки пользователи не могут выполнять такие повседневные задачи, как проверять почту, открывать интернет-страницы или другие интернет-ресурсы.

- ***Фишинг***. Кибератака, при которой злоумышленники посредством различных каналов, например электронной почты, SMS-сообщений, телефонных звонков, социальных СМИ и тактики социальной инженерии, обманом заставляют жертв поделиться чувствительной информацией, такой как пароли или номера счетов. Фишинг часто используется для распространения вредоносного программного обеспечения.

Baltic Centre for Media Excellence
Google

- ***Атака путем подмены участника.*** В этом случае злоумышленники подменяют доверенные источники, например, домены электронной почты или интернет-страницы, чтобы ввести жертву в заблуждение. Как правило, такие атаки нацелены на кражу информации, вымогательство или установку на устройства вредоносного программного обеспечения.

Как защититься?

Цифровая безопасность организации в большой степени зависит от осведомленности сотрудников о различных рисках, от доступных ресурсов и общего уровня подготовленности, включая «цифровую гигиену» – постоянное следование привычкам, снижающим риски кибератаки. Залог кибербезопасности – наличие знакомой пользователям системы информационных и коммуникационных технологий организации. Помните, что во время кризиса будет доступно только оснащение и протоколы, установленные до него. Мы составили 9 вопросов, которые помогут вам подготовиться и хладнокровно встретить кризис кибербезопасности.

1. Проводилась ли оценка рисков?

Каждая организация сталкивается с присущими именно ей рисками цифровой безопасности, которые зависят от ее масштаба, целей, деловых партнеров, используемых ИТ-продуктов и услуг. Критически важно провести оценку используемого в работе оснащения и программного обеспечения, определить, кто имеет к ним доступ, идентифицировать хранилище электронной почты и установить, как сотрудники получают доступ к своей почте. Помимо этого, организации следует выявить сферы деятельности, связанные с потенциальными угрозами ИТ-продуктам и услугам, например, как организовано администрирование и поддержка сервера веб-страницы – своими силами или в виде сторонней услуги. Чтобы снизить вероятность атаки и смягчить возможные последствия, каждый ИТ-продукт, услугу и сопутствующий вид деятельности нужно подвергнуть отдельной оценке рисков. Необходимо проводить регулярные проверки, в том числе делать регулярный анализ риска и обзор принятых мер безопасности и протоколов.

2. Вы храните данные и делаете резервные копии?

НЕСГИБАЕМАЯ ПРИБАЛТИКА

Одна из наиболее серьезных угроз цифровой безопасности связана с возможностью потери, искажения или временной недоступности данных организации. Чтобы уменьшить этот риск, крайне важно использовать понятную и надежную систему хранения и резервного копирования данных. Организация должна определить, какие данные хранятся, а также – где и кто из сотрудников имеет к ним доступ. Важно отметить, что кибератаки часто нацелены на резервные копии корпоративной сети, поэтому их нужно хранить в отдельной среде, отключенной от основной сети. Кроме того, в случае кризиса жизненно важно предоставить всем сотрудникам удаленный доступ к необходимым данным, возможно, посредством облачных технологий.

3. Знаком ли персонал с цифровой гигиеной?

Независимо от вложений в продукты и услуги информационных технологий, фактическая безопасность данных, систем и оснащения организации зависят от понимания ее сотрудниками принципов цифровой гигиены. Умение сотрудников распознавать угрозы на уровне пользователя существенно повышает безопасность организации в целом. Важно проводить регулярное обучение персонала, чтобы повысить осведомленность о цифровой гигиене. Если у организации нет ресурсов для проведения таких тренингов, существуют различные учреждения, помогающие организациям публичного сектора в информировании об ИТ-безопасности.

Как соблюдать цифровую гигиену:

- ***Обновляйте программное обеспечение.*** Следите за обновлениями программного обеспечения своих компьютеров и телефонов в соответствии с рекомендациями производителя. Скачивайте обновления только из надежных источников, например – из магазинов приложений App Store или Google Play.

- ***Регулярно удаляйте неиспользуемые приложения.*** Удаляйте из смарт-устройств и компьютеров приложения и программы, которые больше не используются, чтобы снизить потенциальные риски безопасности.

- ***Персонализируйте разрешения приложений.*** При установке на телефон нового приложения проверьте, к каким данным оно запрашивает доступ, и оцените целесообразность этого. Например, подумайте, зачем приложению Instagram доступ к вашему списку контактов или микрофону, если вы не пользуетесь этими функциями.

- ***Будьте осторожны с незнакомыми электронными письмами.*** Проверяйте подлинность писем от неизвестных отправителей. Если что-то в электронном письме выглядит подозрительным, будьте настороже.

- Остерегайтесь подозрительных вложений и ссылок. Не нажимайте на ссылки и не открывайте вложения в подозрительных электронных письмах и письмах от незнакомых отправителей, поскольку это может быть фишинговая атака. Получив такое письмо, переключите в меню настроек письма HTML в текстовый формат, чтобы увидеть подлинный источник ссылок и отключить автоматическое выполнение скриптов третьих сторон.

- Меняйте пароли. Регулярно обновляйте пароли и старайтесь не использовать один и тот же пароль на нескольких платформах. Для безопасной организации своих паролей используйте бесплатные менеджеры паролей, например Bitwarden или Keepass. Создавая новый пароль, постарайтесь, чтобы он содержал комбинацию букв, цифр и символов. Для дополнительной безопасности используйте необычные комбинации, которые трудно угадать (например, TainstvennijJenot21).

- Везде, где это возможно, используйте двухфакторную аутентификацию. Используйте приложения, например Google Authenticator, которые обеспечивают дополнительную степень безопасности, запрашивая уникальную комбинацию цифр, помимо пароля, при входе в ваш профиль.

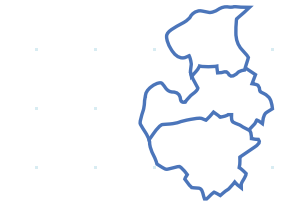
4. Кому предоставлены права администратора различных систем и устройств?

Приобретенное организацией оборудование, включая компьютеры, мобильные телефоны, фотокамеры, и программное обеспечение являются собственностью организации. Поэтому данные системы должны управляться централизованно и использоваться исключительно для рабочих задач. Обеспечить это поможет назначение одного из сотрудников ответственным за управление и контроль ИТ-инфраструктуры предприятия. Он должен проводить регулярное сервисное обслуживание и обновление ИТ-активов. Кроме того, он будет обязан обучать персонал кибербезопасности и следить за соблюдением установленных процедур цифровой безопасности. Это включает в себя внедрение требований относительно сложности паролей, запрет на повторное использование паролей, рекомендацию использовать двухфакторную аутентификацию, где это возможно, и другие необходимые практики безопасности.

5. Как сотрудники заходят на платформы социальных СМИ и в электронную почту?

Неотъемлемой частью работы в индустрии СМИ является использование различных платформ для онлайн-общения и социальных сетей. Доступ к этим платформам осуществляется не только

с рабочих компьютеров, но и с личных устройств, например телефонов. Крайне важно, чтобы каждый сотрудник создавал уникальные имена пользователя и пароли для своих учетных записей, а для дополнительной безопасности включал двухфакторную аутентификацию при входе в систему. Возможности двухфакторной аутентификации предлагает ряд приложений и сервисов, например Google Authenticator или Microsoft Authenticator. Важно выбрать инструмент или сервисное предприятие, наиболее соответствующее потребностям и возможностям вашей организации.



6. Как происходит обмен и совместное использование данных?

Организации часто подвергаются кибератакам через вредоносные электронные письма, стремящиеся получить доступ к данным и информации организации. Для дополнительной безопасности рекомендуется шифровать обмен данными – в особенности электронные письма. Шифрование преобразует содержание письма из простого текста в зашифрованный, доступный только указанному получателю. Данная функция, предоставляемая такими сервисами, как подписка Microsoft 365, помогает защитить чувствительную информацию. Например, рекомендации по повышению безопасности электронной почты разработало Американское агентство по защите кибербезопасности.

7. Какие каналы коммуникации используются для каждой цели?

Организации и их сотрудники ежедневно используют разные каналы связи, например: электронную почту, приложения для обмена сообщениями и др. При составлении планов устранения разных видов кризисов важно заранее определить и согласовать каналы коммуникации, которые будут использоваться в кризисной ситуации. Необходимо разработать понятное руководство по наделению правами администратора канала, предпочтительно – минимум двух заслуживающих доверия сотрудников. Во время кризиса рекомендуется обеспечивать персоналу доступ минимум к двум каналам связи: одному основному, который обычно используется в повседневной коммуникации, и второму резервному в другом приложении-мессенджере. Это обеспечит непрерывность обмена информацией даже в случае технических неполадок в основном канале связи. Такой кризисный протокол действий должен предусматривать, когда и как будет использоваться каждый канал связи, чтобы обеспечить быстрое и эффективное распространение информации.

8. то должны делать сотрудники в случае кибератаки?

Кибератаки проявляются в разных формах, и зачастую люди не замечают, что их компьютер, электронная почта или мобильный телефон уже скомпрометированы. Чтобы усилить осведомленность и оперативность реагирования сотрудников, организации должны создать атмосферу, поощряющую информировать о подозрительных электронных письмах, необычных сообщениях в мессенджерах или странном поведении устройств. Критически важно, чтобы сотрудники сообщали о своих подозрениях, не опасаясь осуждения или насмешек, даже если опасения окажутся необоснованными.

Разработка протокола информирования, подробно описывающего, как и кому следует сообщать о подозрениях, поможет систематизировать и упорядочить этот процесс. Чем свободнее сотрудники выражают свои опасения, тем проще ответственному лицу выявлять риски и обеспечивать кибербезопасность организации.

НЕСГИБАЕМАЯ ПРИБАЛТИКА

9. Вы готовы реагировать?

Разработайте протоколы действий, разъясняющие, что должны делать сотрудники в случае угрозы ИТ-продуктам и услугам организации вследствие кибератаки или другого кризиса (например, наводнения или пожара). Регулярно обновляйте эту информацию и проследите за тем, чтобы все сотрудники хорошо знали кризисные процедуры.

Цифровая безопасность в случае кризиса

Если кризис вызван покушением на продукты и услуги информационных технологий организации, например кибератакой или утечкой данных:

1. Определите масштаб ситуации. Быстро оцените объемы кризиса и изолируйте скомпрометированные продукты и услуги информационных технологий, чтобы не допустить распространения ущерба.
2. Оповестите сотрудников. Сообщите сотрудникам о кризисной ситуации и дайте конкретные указания о том, что нужно сделать для ее устранения.
3. Изолируйте скомпрометированное оборудование. Отключите скомпрометированное оборудование от корпоративной сети, чтобы ограничить влияние атаки.
4. Проанализируйте ситуацию и составьте план восстановления. Проведите расследование атаки или утечки данных, чтобы выявить причину, и разработайте всеобъемлющий план восстановления. Активируйте кризисный протокол и приведите его в соответствие с конкретной ситуацией.

Если кризис не связан с покушением на продукты и услуги информационных технологий организации:

1. Активируйте утвержденные внутренние каналы коммуникации. Используйте только внутренние каналы коммуникации, указанные в кризисном протоколе.
2. Следуйте рекомендациям. Обеспечьте соблюдение рекомендаций, указанных в пунктах 2, 3, 5 и 6.
3. Проверьте безопасность данных. Подтвердите наличие необходимых данных на облачных платформах и обеспечьте доступ к резервным копиям.
4. Защитите критически важные ресурсы: примите меры по защите критически важных ресурсов организации в условиях кризиса.

Автор: Зане Штала (Zane Štāla)
Редактор: Криста Приедите (Krista Priedīte)

Baltic Centre for Media Excellence
Google