На сайте Минсвязи создан специальный раздел "Кибербезопасность"

Предлагается ознакомиться с материалом, подготовленным специалистами РУП "Белтелеком": Современные аспекты кибербезопасности

В современном мире наблюдается активное развитие, внедрение и совершенствование электронных информационных систем, автоматизация множества процессов.

В условиях развития цифровой экономики информационный ресурс стал одним из наиболее мощных рычагов экономического развития. Своевременное владение актуальной информацией – залог успеха в любом виде хозяйственной деятельности.

При этом, наряду со стремительным развитием компьютерных технологий, обострилась проблема защиты информации, несанкционированный доступ к которой может привести к причинению материального вреда и иным негативным последствиям.

Развитие современных информационных и компьютерных технологий всегда отражается практически на всех сферах жизнедеятельности общества, а их повсеместное использование приводит не только к повышению уровня жизни общества, но и к росту числа совершаемых преступлений в сфере компьютерной информации.

Проблемы, связанные с противодействием киберпреступности, являются чрезвычайно важными. Все чаще под ударами кибератак оказываются различные организации, как государственной, так и частной формы собственности, а также граждане республики.

Одной из актуальных проблем на сегодняшний день остается хищение денежных средств субъектов хозяйствования путем несанкционированного доступа к системам дистанционного банковского обслуживания, электронным почтовым ящикам, а также путем заражения компьютеров вредоносным (шпионским) программным обеспечением.

Несанкционированный доступ к компьютерной информации, позволяющий совершать хищения денежных средств, в том числе виртуальных, может осуществляется различными способами. Самими распространенными из которых выступают: «фишинг» и «фарминг».

Фишинг представляет собой способ несанкционированного доступа к конфиденциальным данным пользователя посредством электронных писем или СМС-ссылок, содержащих адрес на подставной сайт-близнец, или загрузки вредоносного программного обеспечения.

Фарминг один из самых прогрессирующих и опасных видов атак, базируется на процедуре внедрения вредоносного кода на персональный компьютер пользователя или сервер, который автоматически производит замену оригинального ip-адреса на поддельный.

В основе указанных методов лежит обман пользователя в целях завладения логинами и паролями для доступа к аккаунтам различных Интернет-сервисов, а также открытыми и приватными ключами, кодовыми словами для входа в электронные почтовые ящики и

криптокошельки.

Механизм работы «фишинга» включает 2 основных способа доступа к конфиденциальным данным: собственноручный ввод данных на поддельных сайтах или загрузка вредоносной программы. Указанные способы реализуются посредством спам-рассылки писем преимущественно через электронную почту. В них содержатся указания, необходимые для выполнения под угрозой негативных последствий (штрафные санкции и т.д.).

Такие письма содержат ссылку, ведущую на сайт, где необходимо ввести личные данные, либо включает в себя автоматическую загрузку вредоносного программного обеспечения, которое, помимо прочего, может быть внедрено во вложение к электронному письму. Попадая на устройство, вирусная программа осуществляет заложенные в ней функции (считывает вводимые либо уже сохраненные данные на компьютере).

В свою очередь, «фарминг» представляет собой достаточно сложный механизм, суть которого заключается в подмене ip-адреса интернет-страницы или на созданную злоумышленниками его копию на взломанном сервере.

Владельцами данных сайтов являются крупные организации и предприятия, обеспечивающие безопасность своих страниц. Порой злоумышленникам удается обойти защиту и получить доступ к конфиденциальной информации как самой организации, так и ее клиентов.

Для Республики Беларусь наиболее характерен такой метод хищения денежных средств субъектов хозяйствования как «фишинг».

Обнаружить попытку фишинговой атаки не сложно, если обладать базовой компьютерной грамотностью и уделять должное внимание анализу и проверке электронных писем, посещаемых сайтов и веб-страниц. Необходимо обращать внимание на URL-адрес ресурса, поскольку при фишинге адрес отличается на 1-2 буквы, цифры или 1-2 символа. Получая электронные письма, следует анализировать не только содержимое, но и отправляемое. Для получения знаний по способам анализа электронных писем, посещаемых сайтов и веб-страниц РУП «Белтелеком» оказывает услугу: «Повышение осведомлённости в сфере информационной безопасности». Указанная услуга предоставляет возможность пользователям систем организации, без отрыва от производственного процесса, сформировать и закрепить навыки безопасной работы в цифровой среде. Прошедшие обучение в последствии делятся приобретёнными знаниями со своим окружением, что способствует повышению общего уровня цифровой грамотности организации.

Обычно письма содержат призывы к активным действиям пользователя (представить адресату конфиденциальные данные, произвести оплату за товар, услуги, в том числе на новый расчетный счет).

На сегодняшний день лучшими методами защиты является шифрование, антивирус, брандмаузер, цифровые подписи, двухфакторная аутентификация и использование различного программного обеспечения, которое способно в автоматическом режиме сканировать систему на наличие вирусов и попыток внедрения новых вредоносных программ. В этой связи РУП «Белтелеком» внедрены и оказываются следующие услуги: защита от DDoS атак, фильтрация сетевого трафика, предоставление лицензий антивирусного программного обеспечения и родительский контроль.

Повышенная угроза и степень распространения атак побуждают к принятию активных действий по формированию мер предупредительного характера. Первым шагом создания

киберзащиты является понимание того, насколько организация подвержена риску атак, и определение уязвимостей, которые должны быть устранены.

Также необходимо понимать, что злоумышленник не сможет достичь своей цели и похитить денежные средства, если атака будет вовремя выявлена, а это возможно на любом ее этапе, при своевременном принятии соответствующих мер защиты.

Вместе с тем, следует понимать, что абсолютной безопасности не существует и для эффективного противодействия активно развивающейся киберпреступности важно не скрывать произошедшие инциденты, а участвовать в обмене информацией об атаках и незамедлительно сообщать о них в правоохранительные органы.

**Информация подготовлена специалистами РУП "Белтелеком"*
