КАК ЗАЩИТИТЬ ПРЕДПРИЯТИЕ ОТ КИБЕРУГРОЗ

ОСНОВНЫЕ СХЕМЫ КИБЕРУГОЗ

В последнее время в области регистрируются киберпреступления, направленные на завладение денежными средствами субъектов хозяйствования, в том числе, государственных предприятий Республики Беларусь.

Хакеры заранее планируют и получают несанкционированный доступ к данным организации, превращают их в беспорядочный набор символов и предлагают расшифровать их после перечисления денежных средств на указанный счет.

К примеру, в июле на электронную почту предприятия в Витебске поступило письмо с вложением. Название вложения вызывало желание открыть этот файл, так как обещало скидки на предлагаемый товар. После скачивания данного файла информация, содержащаяся на ПЭВМ, зашифровалась, а на экране высветилось сообщение с предложением за расшифровку файлов перевести денежное вознаграждение на указанный криптокошелек.

Бывает так, что цель хакеров – получить доступ к конфиденциальной информации, но чаще всего атакующих интересуют деньги.

Может использоваться взломанная электронная почта предприятия-партнера, тогда злоумышленники продолжают переписку с сотрудником предприятия или организации с целью завоевать его доверие и убедить выполнить некоторые действия в интересах самих злоумышленников.

К примеру, в сентябре 2022 года на электронный почтовый ящик сотрудника одного из предприятий г. Витебска поступило электронное письмо от партнера из Кореи, к почте которого получен несанкционированный доступ. Письмо содержало информацию об изменении расчетного счета и информацию об образовании дочернего предприятия. Также письмо содержало требование оплатить доставку товара на новый расчетный счет. В последующем, данный сотрудник подготовил дополнительное соглашение, содержащее измененные реквизиты счета для оплаты товара, а в октябре 2022 года денежные средства в сумме ***более 24 420 долларов*** *зачислены на расчетный счет злоумышленника, открытый в банковском учреждении Китая.*

Также мошенники могут использовать адрес, который визуально похож на официальный адрес субъекта хозяйствования или его партнера, но отличается на несколько символов.

Например: «kula@telliko.com», вместо «kula@teliko.com».

Зачастую преступление состоит из нескольких этапов.

В декабре 2022 года злоумышленники создали фишинговый сайт нефтеперерабатывающего предприятия, внешне аналогичный оригинальному, зарегистрировали его с похожим Интернет-адресом и от имени белорусского предприятия вели переговоры с заинтересованными о поставках несуществующих продуктов переработки, не имея на то возможности. В итоге, получили деньги на подконтрольные им счета.

Планируя кибератаку, злоумышленники прежде всего рассчитывают на человеческие ошибки и слабости, а не на уязвимость программного обеспечения, которую гораздо сложнее преодолеть. Злоумышленник сначала изучает предполагаемую жертву, собирает необходимые данные, затем переходит к завоеванию доверия, вынуждая жертву неосознанно нарушить правила безопасности: предоставить доступ к компьютерным сетям, клиентским базам, базам данных, разработкам или программному обеспечению или раскрыть конфиденциальную информацию.

Необходимо понимать, что злоумышленник не сможет достичь своей цели и похитить денежные средства, если атака будет своевременно выявлена и остановлена, а это возможно на любом ее этапе при принятии соответствующих мер защиты, направленных на сохранение благосостояния, в том числе при соблюдении работниками следующих правил:

1. **обеспечивать должный уровень информационной безопасности** в соответствии с развитием и обновлением программного обеспечения, а также нормативно-правовыми актами Республики Беларусь (**Указ «О кибербезопасности» от 14.02.2023 №40**);

2. **регулярно осуществлять резервное копирование** важных данных;

3. **никогда не доверять отправителю электронного письма**, перепроверять указанную информацию, а также основные идентификационные данные и служебные заголовки электронных писем (можно узнать и проанализировать ip-адрес отправителя письма и иную необходимую информацию), прежде чем ответить на письмо, даже если вам пишет давний партнер с нового адреса;

4. **не переходить по ссылкам и не открывать вложения**, если отправитель письма не тот, кем он представился;

5. в случае изменения реквизитов расчетного счета партнера, **устанавливать данный факт по любым другим каналам связи** (лично, по телефону и т.д.);

6. **использовать ключ ЭЦП (электронной цифровой подписи) непосредственно при работе** с соответствующим программным обеспечением, извлекать его из USB-порта после окончания работы;

7. **тщательно проверять адрес сайта;**

ıписям, в том числе при
ика;

чем ввести персональные
ы доступа, финансовые

ировать счета в случае
:е;

ную информацию.

иводействию киберпреступности
и УВД Витебской облисполкома