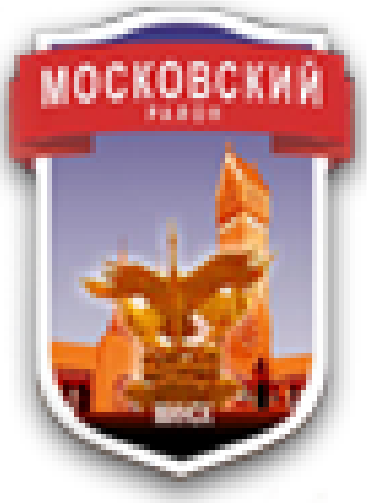


(/)

Администрация Московского района г.Минска

(/)

Как защитить предприятия от киберугроз? Отвечает управление «К»

Более 100 белорусских субъектов хозяйствования в прошлом году пострадало от киберпреступлений. Санаторий, мясокомбинат, торговый дом, жилищно-коммунальная организация, спортивный центр, медицинское учреждение, районная администрация, туристическое агентство, добывающий завод... Список «жертв» впечатляет разнообразием родов деятельности, форм собственности и штатной численности, а сумма ущерба исчисляется сотнями тысяч рублей. Заместитель начальника управления по раскрытию преступлений в сфере высоких технологий Министерства внутренних дел Кирилл Вяткин рассказал, о каких злодеяниях против информационной безопасности предприятий стоит знать всем без исключения работникам – от рядовых сотрудников до высокого руководства.

Способы совершения киберпреступлений в отношении субъектов хозяйствования во всем мире примерно одинаковые. К одному из самых распространенных относится шифрование коммерческой информации, хранящейся на компьютерном оборудовании и в локальных сетях. Атака может происходить путем взлома существующих учетных записей пользователей, которые в силу служебных обязанностей с помощью специальных программ имеют удаленный доступ к данным организации. Таким образом злоумышленники получают возможность внедрения вирусного программного обеспечения в компьютерную систему юридических лиц, превращающего всю документацию в бесполезные файлы с абракадаброй. На рабочих столах ПК хакеры оставляют письмо примерно следующего содержания: «Чтобы получить доступ к зашифрованной информации и продолжить финансово-хозяйственную деятельность в нормальном режиме, перечислите такую-то сумму в криптовалюте на такой-то кошелек».

Еще один сценарий, который может привести к аналогичному исходу, не связан с непосредственной атакой на серверы предприятия. Преступникам будет достаточно лишь отправить на электронную почту учреждения под видом коммерческого предложения, проекта договора или любого другого документа так называемое «фишинговое» письмо с вложением-вредоносом. Двойной щелчок левой кнопкой мыши – и ничего не подозревающий получатель своими руками запускает необратимый процесс превращения ценной для компании информации в бесполезный набор символов.

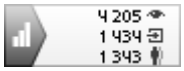
«Важно понимать, что самое главное для любого юридического лица – как можно скорее наладить работу, поэтому многим проще выполнить требования вымогателей, чтобы оперативно вернуть все на круги своя. В то же время нет никаких гарантий, что после перечисления средств доступ к данным будет восстановлен. Так, в ряде случаев заявления в милицию от организаций поступают, когда деньги уже заплатили, а желаемого так и не получили», – отметил Кирилл Александрович.

Не теряет популярности и другая криминальная схема. Ее используют, когда речь идет о длительных и успешных деловых отношениях белорусской фирмы и зарубежного контрагента. Поскольку механизм взаимодействия между этими структурами четко отлажен, а эффективное сотрудничество длится много лет, уровень доверия очень высок. Так как субъекты хозяйствования находятся в разных странах, личные встречи их представителей случаются редко, зато они активно контактируют по электронной почте. Злоумышленники получают доступ к одному из ящиков, участвующих в переписке, и какое-то время, что называется, прощупывают почву, изучая ситуацию. К активным действиям они переходят, когда у компаний намечается крупная сделка на сумму со многими нулями. Чтобы завладеть деньгами, со взломанного email предприятия (или же другой электронной почты с максимально похожим адресом) хакеры высылают письмо, в котором от имени юрлица уведомляют партнеров об изменении реквизитов для перевода средств, например, в связи с техническими неполадками в банке или заморозкой прежних расчетных счетов. Для

убедительности к посланию прилагают соответствующие документы. Они, конечно, фальшивые – с искусно подделанными в графическом редакторе печатью и подписью. Заметить следы монтажа можно только при тщательном рассмотрении файлов в специальной программе. Естественно, у получателей нет никаких оснований сомневаться в достоверности этой информации. Правда выясняется, лишь когда перечисливший деньги контрагент начинает предъявлять претензии по поводу неисполнения договорных обязательств.

Как же защитить субъекты хозяйствования от киберугроз? «Информационная безопасность на предприятиях и в организациях, особенно крупных, должна быть поставлена во главу угла. Обеспечивать ее необходимо так же обстоятельно, как и экономическую. В этой сфере важно выработать четкую политику и принять жестко регламентирующие ее документы, которые закрепят меры по борьбе не только с гипотетическими киберпреступными посягательствами из вне, но и возможной «подрывной деятельностью» внутри организации, к примеру, в пользу конкурентов. Уделять внимание данным вопросам нужно регулярно, а лучше всего отдать их на откуп профессионалам – заключить договор с компанией, оказывающей такие услуги, или же ввести соответствующие должности в собственный штат. Кроме того, обязательно регулярно выполнять резервное копирование данных, а также пользоваться актуальными антивирусами и специализированным программным обеспечением, которое блокирует таргетированные атаки», – резюмировал Кирилл Вяткин.

Заместитель начальника УРПСВТ МВД Республики Беларусь
Кирилл Вяткин

КУП «Центр информационных технологий Мингорисполкома» (http://it-minsk.by/ru/) © 2001-2023


(https://metrika.yandex.ru/stat/?id=25870868&from=informer)