ИТ-СЕКТОР

Как защитить свой бизнес

от кибермошенников

Последние годы в Беларуси регулярно появляются новости о кибератаках на крупные компании, утечках данных и взломах сайтов. Параллельно увеличиваются расходы бизнеса и госсектора на кибербезопасность. По некоторым подсчетам, емкость рынка кибербезопасности нашей страны составит более 100 млн USD в 2026 г. Активно идет создание регуляторной базы, вопросы информационной безопасности обсуждаются на форумах и конференциях. Так, на недавнем Международном ИКТ форуме «ТИБО» этой теме тоже уделили внимание.

«ЭГ» решила внимательнее изучить, какие проблемы наиболее остро стоят сейчас перед компаниями, как они могут бороться с хакерскими атаками и зачем им постоянно учить своих сотрудников. Для этого мы поговорили с экспертом по информационной безопасности из РФ, руководителем отдела развития продуктов компании «АйТи Бастион» **Константином Родиным**.

– Константин, на ваш взгляд, какие проблемы, связанные с обеспечением информационной безопасности, несут самую большую угрозу бизнесу и госсектору Беларуси? Отличается ли ситуация в нашей стране и в России?

– Ситуация с информационной безопасностью в Беларуси очень схожа с российской: планомерный процесс повышения инфобеза в частных и государственных компаниях прервался из-за массового бегства иностранных вендоров. Очень многие организации, как в России, так и в Беларуси, делали ставку на мировые компании и их решения: люди учились годами, привыкали к оборудованию и ПО, выстраивали внутренние процессы. Соответственно, после ухода с рынка иностранных вендоров появились сложности с продлением лицензий, получением технической поддержки. И сейчас четко сформировался тренд на переориентацию рынка на отечественные решения.

Еще одна острая проблема – в разы увеличилось количество противоправных действий в отношении самых разных компаний. Сливы, утечки данных, падение инфраструктуры компаний происходят по всему миру. Но своя рубашка ближе к телу, поэтому проще говорить про наш регион. Здесь основная проблема заключается в том, что никто не был готов к такому количеству атак. При этом ситуация понемногу стабилизируется. Беларуси в этой части даже проще: есть тесное сотрудничество с Россией, а значит, возможность не наступать на те же грабли. Я знаю, что сейчас ваш ОАЦ активно сотрудничает с ФСТЭК России, с российскими компаниями. В последнее время в Беларуси сделаны важные шаги для улучшения ситуации – например, начал работать Указ от 14.02.2023 № 40 «О кибербезопасности», который призван обеспечит базовые принципы построения центров информационной защиты. На мой взгляд, этот документ хорошо проработан, дает понимание, в какую сторону двигаться, и предлагает конкретные решения.

– Как вы уже отметили, большое количество белорусских компаний работали и работают до сих пор с ПО иностранного производства. И после введения санкций есть много вопросов. Как организациям выходить из сложившейся ситуации?

– Как представитель компании-вендора, я бы сказал, что нужно срочно менять все ПО и все внедренные решения. Но, если честно, разумнее будет постепенный переход. Не нужно рушить выстроенные процессы, лучше поэтапно осваивать другие решения. Это позволит и сэкономить бюджеты, и плавно перестроить процесс работы.

– Может ли ваша компания предложить альтернативу?

– «АйТи Бастион» сейчас производит два продукта. Первый называется СКДПУ НТ – это система контроля доступа привилегированных пользователей (eng. PAM). По сути это система, которая позволяет пользователю подключиться к серверам, сетевому оборудованию, рабочим станциям или базам данных. И при этом компания и офицеры безопасности получают данные о том, какие действия производились этим пользователем при подключении. Если упрощать – это стенографистка, которая записывает все, что вы вводите, плюс еще и оператор с камерой, который записывает ваши действия.

Помимо сбора информации, мы еще анализируем поведение пользователей. Например, злоумышленник получил логин и пароль от PAM-системы (купил их в даркнете). В его руках оказалась, допустим, учетная запись бухгалтера, и он начал совершать действия, не характерные для такого специалиста. Для нас это сигнал, что надо предпринимать меры. Сейчас есть довольно много решений, которые занимаются непосредственно реагированием, но они стоят дорого. В свой продукт мы включили минимальный набор функций для того, чтобы быстро среагировать и остановить злоумышленника. Это сильно сокращает время его нахождения в системе и минимизирует вред.

О компании

Российская компания «АйТи Бастион» разрабатывает средства защиты информации. В отрасли информационных технологий и информационной безопасности работает с 2014 года. Технологии «АйТи Бастион» сертифицированы ОАЦ РБ и вписываются в программы импортозамещения ПО на особо значимых объектах.

– Какие проблемы решает второй ваш продукт?

– На многих предприятиях есть изолированные сегменты сетей, которые обрабатывают данные для служебного пользования. Зачастую обмен информацией между такими закрытыми сегментами идет через USB-накопитель. В одном контуре информацию накопили, на флешку записали, и специально обученный человек понес ее к компьютеру в другом закрытом контуре. Это рабочий сценарий, но медленный, нередко подразумевающий заполнение журналов от руки о приемке-передаче той самой флешки. И в нем присутствует человек, который до сих пор является самым уязвимым звеном в любой системе инфобеза. Наш программный комплекс «Синоникс» позволяет обеспечить контролируемый и автоматизированный информационный обмен между сетями. Он будет интересен банкам, промышленным предприятиям, силовым структурам, научно-исследовательским институтам – всем, кто работает с чувствительной информацией для служебного пользования.

– Нужно ли адаптировать ваши решения для белорусского рынка?

– Нет, я не вижу никаких различий в процессе внедрения или эксплуатации наших продуктов в РБ и РФ. Есть определенная разница в регуляторной базе, но в целом она похожа во всем мире. Дополнительных усилий или затрат от белорусских заказчиков не потребуется.

– Вы сказали, что самым уязвимым звеном в системе инфобеза по-прежнему является человек. Могут ли случаи бытовых мошенничеств через мессенджеры, телефоны, фишинговые электронные письма в отношении рядовых сотрудников нести угрозу для компании?

– Начну вот с чего – мои коллеги недавно проводили небольшое исследование. Через открытые источники они находили сотрудников компаний и писали им в личные сообщения просьбу предоставить логин и пароль за деньги. Дешевле всего им удалось купить такие данные за 1000 росс. руб.

Какой вывод можно сделать? Всем компаниям нужно обращать внимание на то, как хорошо знают их сотрудники не только правила информационной безопасности, но последствия нарушений этих правил. Надо повышать уровень осведомленности в части угроз. Что будет, если ты откроешь письмо, где написано «Ты выиграл!», на корпоративном компьютере? Почему нельзя сохранять логин и пароль на рабочем месте? Что может случиться, если ты передашь или продашь логин и пароль? Нужно объяснять последствия, к которым это может привести, и вводить личную ответственность. По моему опыту: как только в компании внедряются программы обучения сотрудников – проблем становится значительно меньше.

Беседовала Анна СВЕТЛОВА

Одним абзацем

В Беларуси планируется ввести обязанность для маркетплейсов информировать об изменениях в своей деятельности, давать обратную связь по жалобам потребителей, размещать необходимые сведения о товаре. Об этом рассказал министр антимонопольного регулирования и торговли Алексей Богданов агентству БЕЛТА. По словам А. Богданова, «то есть сам маркетплейс будет регулятором на своей же площадке. А сегодня он, по большому счету, отдал все на откуп поставщику и производителю».

Страны Балтии 8 февраля 2025 г. отключат свои электросистемы от единой системы с Беларусью и Россией, а с 9 февраля подключатся к европейской электросети. Об этом сообщает российское информагентство «Интерфакс». Стоимость всего проекта составляет 1,6 млрд EUR. Три четверти расходов покрываются из бюджета ЕС. Латвия, Литва и Эстония остаются последними странами Евросоюза, которые еще не присоединились к континентальной европейской сети. Сейчас все три страны Балтии входят в БРЭЛЛ (электрическое кольцо Беларусь-Россия-Эстония-Латвия-Литва), частоту в котором поддерживает российский системный оператор.

Ассоциация профессиональных перевозчиков пассажиров предлагает создать в Беларуси национального оператора такси. Об этом заявила глава ассоциации Екатерина Станкевич в эфире телеканала СТВ. По ее словам, это принесет «огромные поступления в бюджет».

Компания из Турции впервые заключила сделку по закупке сахара на Белорусской универсальной товарной бирже, сообщили в пресс-службе БУТБ. Объем пробной партии составил 136 тонн. До этого турецкие участники биржевых торгов в основном импортировали через биржу пиломатериалы, лом черных металлов и искусственные волокна, а также поставляли промышленное оборудование для агропромышленного комплекса Беларуси.

Генеральная прокуратура инициировала ужесточение законодательства в сфере летнего оздоровления детей и потребовала не допустить функционирование «стихийных» лагерей этим летом. Об этом сообщили в ведомстве. Одно из главных предлагаемых нововведений – работать с детьми смогут только те организации, которые будут включены в специальный реестр.

В мае 2024 г. в Минске купили квартиру с ценой квадратного метра в 3345 USD. Это самый дорогой квадрат среди всех квартир в столице, которые купили в прошлом месяце, сообщает портал Realt.by со ссылкой на данные из Реестра цен на земельные участки. Обошлась она новому владельцу в 280 тыс. USD. Общая площадь квартиры составила 84 кв. м. Находится недвижимость в жилом комплексе бизнес-класса «Парус» на улице Кальварийская, между станциями метро «Молодежная» и «Фрунзенская».

Авиакомпания «Белавиа» запустила чартерный рейс из Минска на «египетские Мальдивы» – курорт Эль-Аламейн, рассказали в пресс-службе перевозчика. Первый чартер был заполнен на 100%. Полетная программа запланирована до 4 октября 2024 г. с перспективой продления до ноября 2024 г. на период осенних каникул. Туры сформированы на 10/11 ночей с вылетами 3 раза в месяц. Виза оформляется в аэропорту по прилете, стоимость 25 USD за человека.