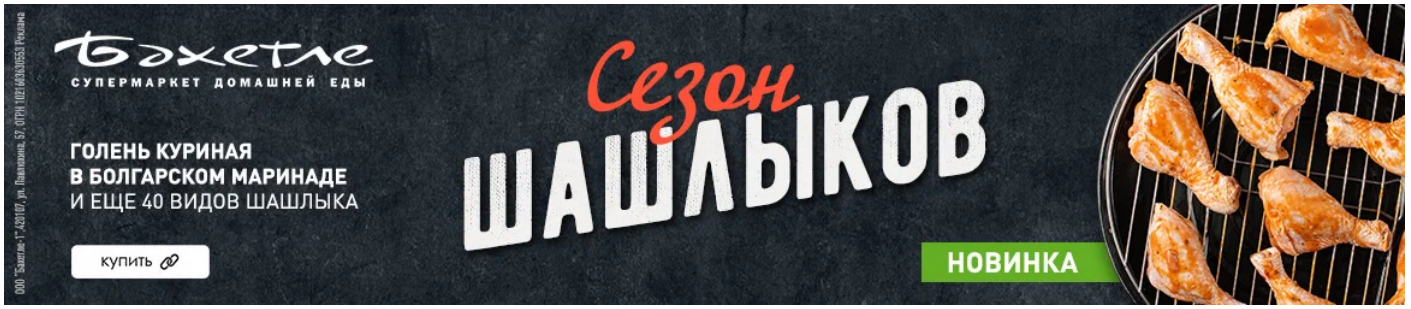


#it #челны

Зарядки для телефонов, удаленный доступ и пароли в даркнете: как хакеры взламывают предприятия Татарстана

13 апреля 2

«Риэль Инжиниринг» о том, как защитить производство технологиями «Лаборатории Касперского»

«Подавляющее большинство организаций в той или иной степени уязвимо перед злоумышленниками», — уверен директор IT-компании «Риэль Инжиниринг» Тагир Ахметзянов. Вместе со своей командой он, используя решения «Лаборатории Касперского», решает вопросы информационной промышленной безопасности на предприятиях.

В текущее время уже немало промышленных предприятий понимает потребность в защите информационной базы. О том, какие угрозы могут быть на предприятиях, как сотрудники могут остановить производство с помощью зарядки для телефона, какие сегменты более всего уязвимы для хакерских атак и кому необходимо заниматься кибергигиеной, — в материале «БИЗНЕС Online».

Руководитель центра по обеспечению информационной безопасности компании Егор Александров

Фото: Олег Спиридонов

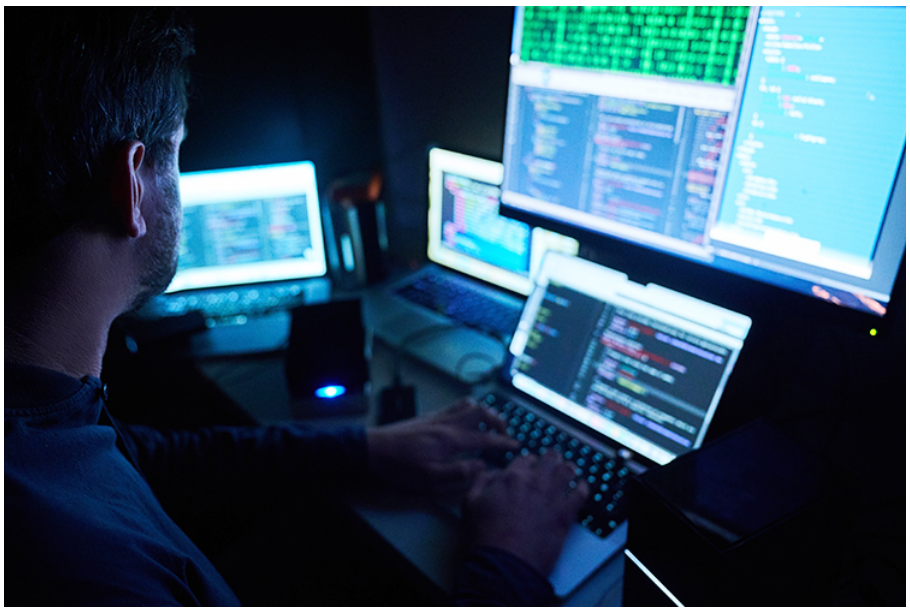
Число инцидентов в кибербезопасности в РФ выросло в 2-3 раза

В России в 2022 году резко увеличилось количество кибератак. За предыдущий год киберпреступники увеличили свою активность. Важность вопроса настолько возросла, что президент России **Владимир Путин** подписал указ №250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации», благодаря которому на руководителей органов и организаций возложили персональную ответственность за обеспечение информационной безопасности.

По данным челнинской IT-компании «Риэль Инжиниринг», которая уже более трех лет стоит на страже кибербезопасности ведущих промышленных компаний Татарстана и России, число инцидентов в сфере информационной безопасности возросло в 2–3 раза по сравнению с 2021 годом. И, как рассказывает руководитель центра по обеспечению информационной безопасности компании **Егор Александров**, в Татарстане ситуация в целом такая же, как и в среднем по стране. А методы атак становятся все изощреннее.

«При этом хакеры часто успешно реализуют и простые атаки. Это связано с тем, что подавляющее большинство организаций в той или иной степени уязвимо перед злоумышленниками», — рассказывает Егор Александров.

По его словам, все более глубокая цифровизация предприятий приводит к необходимости интеграции корпоративного и промышленного сегментов инфраструктуры, появляется дыра, через которую возможно заражение систем управления промышленного оборудования. Раньше два сегмента — корпоративный и промышленный — существовали независимо друг от друга. И проблемы, которые были в одном сегменте, не отражались на другом. А сейчас любой сотрудник, сам того не ведая, может заблокировать работу предприятия одним непродуманным действием. И дело порой доходит до абсурда.



«Хакеры часто успешно реализуют и простые атаки. Это связано с тем, что подавляющее большинство организаций в той или иной степени уязвимо перед злоумышленниками»

Фото: Global Look Press / www.globallookpress.com

Зарядка для телефона, удаленный доступ и другие уязвимости

Например, на промышленном предприятии есть оператор технологической установки. Система автоматизирована, не требует постоянного участия человека в ее работе. Сотрудник за ней просто наблюдает. В один момент он решает зарядить телефон через USB-порт компьютера или контроллера. Сам того не ведая, сотрудник через мобильный интернет своего смартфона открывает злоумышленнику доступ к управлению оборудованием предприятия. Оборудование может быть остановлено, перенастроено, перепрограммировано, а сотрудник при этом даже ничего не заподозрит. «Это все присутствует в реальности, и такие события необходимо непрерывно отслеживать и блокировать», — объясняет директор «Риэль Инжиниринг» **Тагир Ахметзянов**.

Внешние атаки тоже носят различный характер. Одни злоумышленники используют уязвимости внешнего периметра инфраструктуры предприятия, другие атакуют персональные компьютеры и смартфоны сотрудников, а также к набирающим в последнее время активность можно отнести такие угрозы, как несанкционированные полеты БПЛА (дроны).

Директор IT-компании «Риэль Инжиниринг» Тагир Ахметзянов

Фото: Олег Спиридонов

Как защититься от угроз

В целом информационная безопасность это не про «здесь и сейчас», а про профилактику и непрерывные аудиты. Как говорится, поздно пить боржоми, когда почки отвалились.

Насколько общая эффективность предприятия определяется качеством построения и адаптации его бизнес- и производственных процессов, настолько и общий кибериммунитет определяется качеством внутренних регламентов и дисциплиной их соблюдения, а также оперативностью реагирования на выявленные уязвимости в собственной инфраструктуре и на других предприятиях. Необходим непрерывный процесс выявления, реагирования и профилактики.

Огромный вклад в такую работу оказывает регулятор — Федеральная служба по экспортному и техническому контролю (ФСТЭК), которая ведет базу данных выявленных уязвимостей, их классификацию, определение критичности и подготовку рекомендаций по устранению уязвимости. И каждый день эта база данных пополняется десятками, а то и сотнями выявленных уязвимостей. А оборудование и программное обеспечение, в которых они выявляются, пугает своей распространенностью и важностью. Например, всего лишь за один день была выявлена критическая уязвимость в микропрограммах (прошивках) популярных маршрутизаторов, позволяющая использовать маршрутизатор для межсайтовых сценарных атак; в распределенных контроллерных системах управления крупного мирового бренда, позволяющая получить доступ к управлению контроллерами; в популярном web-браузере, позволяющая нарушителю выполнить произвольный код на вашем компьютере; в SCADA-системе, позволяющая получить несанкционированный доступ к внутренней базе данных; в режимах работы популярных графических процессоров, позволяющая нарушителю вызвать отказ в работе оборудования. И все это всего лишь за один произвольный день.

Сейчас недостаточно просто установить антивирусную программу, нужна более комплексная защита. Нужна эшелонированная защита.

Для комплексной защиты промышленной информационной инфраструктуры «Риэль Инжиниринг» использует Kaspersky Industrial CyberSecurity (KICS) — специализированное решение, разработанное «Лабораторией Касперского».

«Риэль Инжиниринг» единственный в Закамье получил статус Platinum Partner «Лаборатории Касперского» — в Татарстане он есть только у трех IT-компаний.

Для комплексной защиты промышленной информационной инфраструктуры «Риэль Инжиниринг» использует Kaspersky Industrial CyberSecurity (KICS) — специализированное решение, разработанное «Лабораторией Касперского»

Фото: Global Look Press / www.globallookpress.com

Как это работает, Тагир Ахметзянов объяснил на примере предприятия ООО «Татнефть-Пресскомпозит», где «Риэль Инжиниринг» внедрил систему KICS. Она помогает предотвратить нежелательные действия пользователей или злоумышленников непосредственно на рабочих станциях и обнаружить аномальные действия в сети, такие как появление новых устройств, сканирование сети, подмена значений тегов промышленных контроллеров.

KICS выделяется тем, что она была разработана специалистами «Лаборатории Касперского» с нуля, с учетом особенностей промышленного оборудования, когда наиболее важной задачей является обеспечение непрерывности производственного процесса. KICS устанавливается и обновляется без перезагрузки оборудования, чтобы не вызывать простои, при работе потребляет мало ресурсов, не загружая машины. «Сбор и анализ сетевого трафика осуществляется на его копии, поэтому негативного влияния на промышленную сеть система не оказывает», — подчеркивает Тагир Ахметзянов.

Продукт KICS конфигурируется строго под конкретный защищаемый объект. «Мы проанализировали архитектуру промышленной сети и определили оптимальное количество точек сбора трафика. Защита конечных станций настроена на каждой производственной машине индивидуально, отдельные функции системы информационной безопасности могут работать как в блокирующем режиме, так и в режиме наблюдения», — рассказывает он.

Решения «Лаборатории Касперского» состоят из двух частей. Первая — защита рабочих станций, серверов, станций операторов. Вторая — это мониторинг и анализ промышленной сети предприятия. Данный компонент собирает трафик, обрабатывает его, разбирает промышленные протоколы, ищет аномалии. И в случае обнаружения какой-либо подозрительной активности оповещает ответственного сотрудника.

Используя в реализации проектов по информационной безопасности различные продуктовые решений от «Лаборатории Касперского», компания «Риэль Инжиниринг» поможет защитить и от таких угроз, как несанкционированные полеты БПЛА (антидрон).

«Риэль Инжиниринг» единственный в Закамье получил статус Platinum Partner «Лаборатории Касперского» — в Татарстане он есть только у трех IT-компаний

Фото: Олег Спиридонов

МУПы тоже представляют интерес для кибермошенников

С компанией «Татнефть-Пресскомпозит» «Риэль Инжиниринг» сотрудничает давно, совместно с заказчиком разработал и внедрил на предприятии автоматизацию и цифровизацию производства по всему циклу — от сырья до испытания готовой продукции. Сегодня это предприятие активно на всех персональных компьютерах сотрудников и промышленных серверах применяет защиту от «Лаборатории Касперского».

Все больше промышленных предприятий понимает, насколько важно внедрять системы промышленной безопасности. Но под угрозой не только они.

«Муниципальные заказчики также представляют интерес для кибермошенников. Особенно в связи со своей однозначной ассоциацией с государством. Но при этом пока большинство МУПов не занимается активно вопросами кибербезопасности, повышения кибериммунитета. А уже давно пора начинать», — констатирует Тагир Ахметзянов.

Большую угрозу представляют собой программы-шифровальщики. Они могут заразить компьютер или сервер, распространиться по всей корпоративной сети, затем затаиться и ожидать момента Х.

Далее при внешней активации киберпреступниками будут зашифрованы все данные на инфицированных компьютерах и серверах — в таком случае предприятие окажется полностью парализовано, остановится работа бухгалтерии, других систем, произойдет полный коллапс. И здесь вопрос общей информационной устойчивости выходит на первый план, имелись ли резервные копии важных данных, насколько быстро оно может восстановиться? Даже если инцидент удастся быстро преодолеть и коллапс не заметит потребитель, его все равно очень сильно заметит предприятие.

А если зашифровать данные серверов и рабочих станций коммунальных служб или получить несанкционированный доступ к их управлению, это может разрушить обеспечение жизнедеятельности города и населения.

Соответственно, рассуждает Тагир Ахметзянов, остановку насосной станции, которая подает воду или откачивает стоки, остановку работы очистных сооружений, котельной, теплоцентрали тут же моментально почувствует весь город, все жители.

«И это не просто какие-то фантазии. Давно известный случай — вывод из строя центрифуг по обогащению урана вирусом Stuxnet в Иране. Это известный пример, который часто приводится. Случаются и остановки насосов крупных промышленных предприятий. Все это реальность, и повторение таких страшных сценариев потенциально возможно», — отмечает он.

Поэтому еще одно важное направление, которым занимается «Риэль Инжиниринг», — кибергигиена

Фото: Олег Спиридонов

Как работает киберразведка

Кроме решений на внутреннем контуре, важный блок — это киберразведка, мониторинг внешнего контура безопасности и так называемого даркнета. «Решения „Лаборатории Касперского“ позволяют получать информацию о том, как злоумышленники видят вас снаружи, какие ваши потенциальные уязвимости могут заметить, чем могут воспользоваться. В процессе анализируются базы данных, базы потенциальных атак, переписка, и, если засвечивается информация о предприятии, утекших паролях и персональных данных, она сразу доставляется до заказчика. Такое бывает нередко», — говорит Тагир Ахметзянов.

Поэтому еще одно важное направление, которым занимается «Риэль Инжиниринг», — кибергигиена. Критически важно повышать осведомленность сотрудников и развивать у них навыки формирования полезных привычек в отношении кибербезопасности, позволяющих не стать жертвой киберугроз и избежать проблем сетевой безопасности.

Ни одна система защиты не сможет обеспечить абсолютную безопасность, считает Тагир Ахметзянов.

В среде специалистов по информационной безопасности есть термин «нулевой день», который относится к уязвимостям, которые еще не были выявлены или публично раскрыты. Поэтому антивирусы, работающие

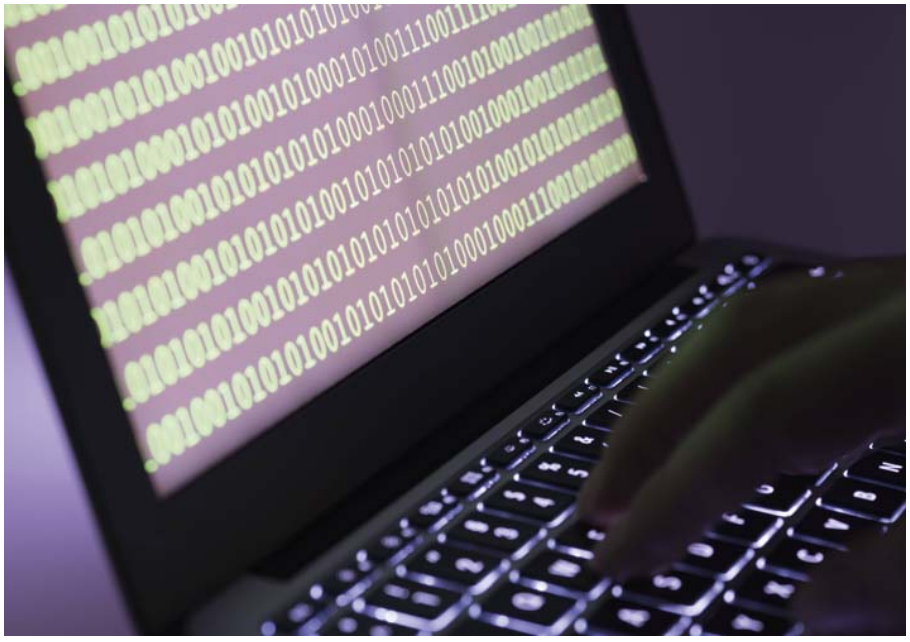
на основе обновляемой базы известных сигнатур вирусов, не смогут распознать и предотвратить работу нового, еще неизвестного вируса.

Более продвинутые продукты информационной безопасности обнаруживают подозрительную нетипичную активность и реагируют на нее.

> Если кто-то раньше считал, что они никакого интереса для злоумышленников не представляли, то сейчас представляют интерес все, в том числе для кражи персональных данных, для кражи информации о банковских карточках и прочее. Сейчас повсеместно понимают, что надо защищаться.
>
> 
>
> Тагир Ахметзянов
> директор IT-компании «Риэль Инжиниринг»

Для этого у «Лаборатории Касперского» есть специальные тренинги по кибергигиене. Например, сотрудникам рассылают фишинговые (поддельные) письма с вредоносной ссылкой, замаскированные под полезную информацию, и проверяется, сколько человек перейдет по этой ссылке. При этом администратор портала видит и может анализировать результаты всех сотрудников.

Также обученные IT-специалисты видят, насколько защищен внешний периметр и внутренняя инфраструктура. Представьте, насколько важно предприятиям заблаговременно узнавать, есть ли у них уязвимости, которые могут быть использованы злоумышленниками, были ли утечки данных и не гуляют ли эти данные в darknet или на хакерских форумах.



Сейчас важнейшим побудительным мотивом для внедрения своей системы кибербезопасности является закон о защите критической информационной инфраструктуры

Фото: Global Look Press / www.globallookpress.com

Государство тоже требует кибераудита инфраструктуры

Сейчас важнейшим побудительным мотивом для внедрения своей системы кибербезопасности является закон о защите критической информационной инфраструктуры. Государство, по словам директора «Риэль Инжиниринг», начало регулировать этот сегмент, оно понимает, что нельзя допустить утечек персональных данных, нельзя допустить остановок критически важных объектов.

«И требует того, чтобы предприятия произвели паспортизацию, инвентаризацию, аудит собственной инфраструктуры на предмет ее рисков и обеспечить надлежащую защиту, и, самое главное, своевременное информирование о произошедших атаках. Для этого существует государственная система — ГосСОПКА (*государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак* — **прим. ред.**), которая все эти данные аккумулирует», — сообщил он.

Обеспечение информационной безопасности критической информационной инфраструктуры не только является насущной необходимостью предприятий для сохранения ритмичности и безостановочности своих производственных процессов и обеспечения своих производственных показателей, но и стало требованием от государства в соответствии с 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», который необходимо исполнять.

IT — информационные технологии
web-браузер — интернет-браузер
SCADA — система диспетчерского управления и сбора данных
Platinum Partner — партнер с платиновым статусом
Stuxnet — Стакснет (название вируса)

Регина Шафиева

Реклама. Риэль Инжиниринг.

Түбән Ешлыклы
13 Апреля 09:19

Из статьи"Ни одна система защиты не может обеспечить абсолютную безопасность " прокомментируйте пожалуста.

ответить

Дихлофос
13 Апреля 10:11

Потому что защита - это воздействие на уже существующую уязвимость.
Превентивные действия не могут охватить все возможные атаки и уязвимости.

ответить

Все комментарии публикуются только после модерации с задержкой 2-10 минут.
Редакция оставляет за собой право отказать в публикации вашего комментария.
Правила модерирования.

Деловая электронная газета «Бизнес Online» (на связи)
Свидетельство о регистрации СМИ Эл №ФС 77-33484 от 15.10.08
Выдано федеральной службой по надзору
в сфере связи и массовых коммуникаций
Учредитель ООО «Бизнес Медия Холдинг»
Шеф-редактор А. В. Брусницын