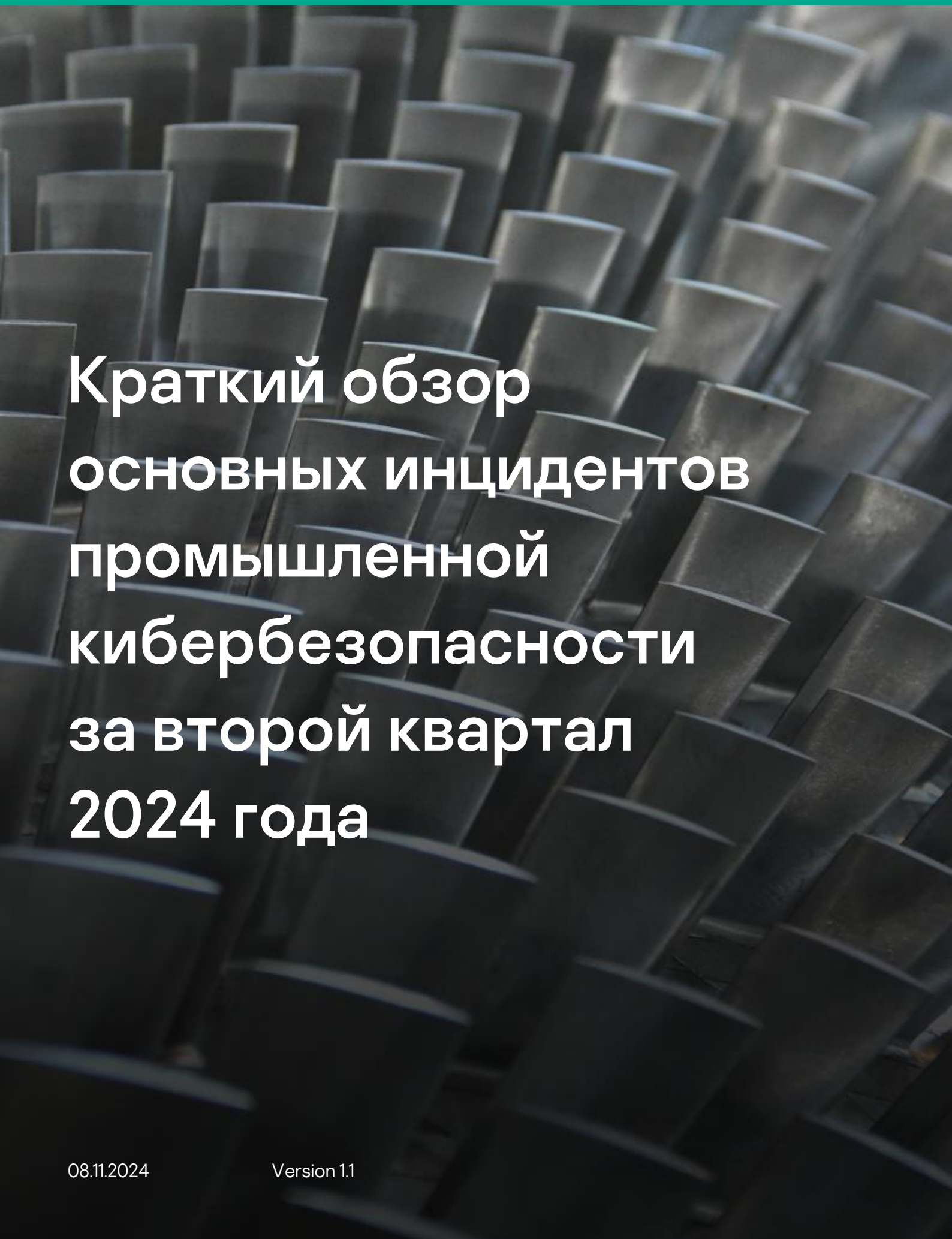
Kaspersky ICS CERT

kaspersky



Краткий обзор основных инцидентов промышленной кибербезопасности за второй квартал 2024 года

08.11.2024

Version 1.1

Общие сведения

Во втором квартале 2024 года жертвами кибератак были публично подтверждены 35 инцидентов. Половина атак привела к нарушению операционной деятельности или поставок продукции. Большинство пострадавших — производственные предприятия, выпускающие продукцию для таких отраслей, как электронная промышленность, автомобилестроение, сельское хозяйство, медицина и строительство. Пострадали также промышленные предприятия других секторов, включая коммунальное хозяйство, транспорт и логистику, фармацевтику и пищевую промышленность.

Насколько можно судить по имеющимся в публичном доступе данным, наибольший ущерб принесла атака с использованием шифровальщика на корпорацию CDK Global, поставщика ИТ-сервисов для американских автодилеров. Атака нарушила работу почти 15 тысяч компаний, что привело к прямым совокупным убыткам в размере 1 млрд долларов. Это не первый и не последний подобный случай. Вне всякого сомнения, в настоящее время кибербезопасности нишевых производителей продуктов и поставщиков услуг, от которых зависит, тем не менее, множество предприятий, уделяется крайне мало внимания. Еще один интересный случай — атака на британского производителя медицинского оборудования LivaNova.

В ходе атаки злоумышленники похитили не только личные медицинские данные клиентов компании, но и серийные номера медицинских приборов. Наши многочисленные исследования уязвимостей свидетельствуют, что некоторые производители устройств интернета вещей (IoT) до сих пор используют серийные номера для генерации ключей шифрования и аутентификационных данных, что упрощает подготовку атак на эти устройства.

К сожалению, даже крупные мировые компании могут иметь уязвимости в безопасности своих продуктов и инфраструктуры, что ставит под угрозу данные клиентов и партнеров, как это было в случае утечки данных из Dell. Конечно, меры по кибербезопасности требуют затрат, и дополнительные инвестиции в защиту неизбежно приводят к увеличению расходов для клиента. Надеемся, что вскоре организации по всему миру начнут признавать недостаточный уровень кибербезопасности своих ключевых технологических поставщиков как один из главных рисков, требующих внимания.

Краткая статистика по кварталу

- Количество публично подтвержденных жертвами кибератак инцидентов по сравнению с первым кварталом 2024 года (30) **выросло на 16%**.
- Почти половина жертв сообщила об **отказе ИТ-систем** (49%) и **нарушении операционной деятельности** (46%). В предыдущем квартале эти показатели составили 43 и 30% соответственно.
- Более половины (51%) жертв сообщили о том, что **подверглись атаке с применением шифровальщика.** В предыдущем квартале об этом заявили 47% жертв кибератак.
- Две трети (66%) жертв относятся к производственному сектору. 57% из них **признались в утечке данных или утечке персональных данных** в результате киберинцидентов.
- Одна компания **не справилась с последствиями кибератаки** и приняла решение о закрытии.
- Наиболее пострадавшие страны:
  - США — 26% (9 инцидентов)
  - Германия — 14% (5)
  - Австралия — 9% (3)
- В числе пострадавших есть такие страны как **Колумбия, Аргентина** и **Израиль**.

Апрель

- LivaNova
- Nexperia
- HOYA
- Swisspro
- Targus
- Taiwan United Renewable Energy
- Le Slip Français
- Octapharma Plasma
- Schuette
- Skanlog
- Tipton Municipal Utilities
- BECOM
- Max Wild
- Dell
- Barnett's Couriers

Май

- Eucatex
- Key Tronic Corporation
- Porto de São Francisco do Sul
- Sawnee EMC
- Lewis Brothers Bakeries
- Lemken
- Wehrle-Werk

Июнь

- Agropur
- Northern Minerals
- Pharmascience
- Iluka Resources
- Westfälische Stahlgesellschaf
- Emcali
- Crown Equipment
- GlobalWafers
- Rekah
- CDK Global
- Sandhar Technologies
- Ocasa
- Meiller Kipper

2024

Производственный сектор

Кибератака на Hoya

Производственный сектор
Утечки данных, отказ ИТ-систем, нарушение отгрузки продукции, нарушение операционной деятельности
Шифровальщики

Японский производитель линз Hoya сообщил об обнаружении 30 марта инцидента с ИТ-системой, который затронул головной офис и несколько бизнес-подразделений. Компания подтвердила факт нарушения работы, несмотря на усилия по изоляции затронутых инцидентом серверов. Она провела расследование, чтобы выяснить, были ли скомпрометированы конфиденциальные или персональные данные, и при поддержке властей постаралась как можно скорее возобновить производство. При этом подразделение Hoya по производству линз для очков сообщило о задержках в доставке заказов. В ходе продолжающегося расследования компания подтвердила, что третья сторона получила неавторизованный доступ к некоторым серверам группы и похитила небольшое количество файлов. Представитель Hoya отказался уточнить, затронули ли перебои в работе компании другие оптические изделия, включая компоненты оборудования для производства микросхем и детали жестких дисков.

Вымогательская группа Hunters International 10 апреля потребовала 10 млн долларов выкупа за программу дешифровки файлов и неразглашение файлов, похищенных во время атаки. 24 апреля Hoya выпустила заявление, подтвердив, что в работе компании и поставках продукции произошли сбои, а из систем компании были украдены некоторые данные. На момент публикации заявления большинство затронутых инцидентом лабораторий снова были открыты.

Атака на Targus с применением шифровальщика

Производственный сектор
Нарушение операционной деятельности
Шифровальщики

Производитель аксессуаров для мобильных устройств со штаб-квартирой в США Targus в своем уведомлении регуляторам сообщил, что стал жертвой кибератаки, которая нарушила его работу после несанкционированного доступа злоумышленников к файловым серверам. Инцидент, обнаруженный 5 апреля, привел к перебоям в работе Targus. Для локализации инцидента компания прибегла к помощи сторонних консультантов по кибербезопасности. Компания уведомила регулирующие и правоохранительные органы, однако не подтвердила факт кражи данных в результате атаки. 19 апреля вымогательская группа Red взяла на себя ответственность за атаку на Targus, опубликовав образец похищенных данных.

Атака на Swisspro с применением шифровальщика

Производственный сектор
Утечка данных, отказ ИТ-систем
Шифровальщики

Швейцарская компания Swisspro, занимающаяся электромонтажом, ИКТ и автоматизацией и входящая в состав группы BKW Building Solutions, подверглась атаке с использованием шифровальщика. В результате пострадала устаревшая ИТ-среда компании, что она подтвердила в своем заявлении местным СМИ. Была создана рабочая группа для оценки влияния и возможных последствий атаки, а также принятия срочных мер, таких как изоляция затронутых систем и смена паролей. Признаки атак на клиентов или другие компании группы BKW не были обнаружены, и Swisspro смогла продолжить предоставление своих услуг. В рамках текущего анализа также была проведена оценка масштаба утечки данных.

Вымогательская группа Black Basta взяла на себя ответственность за инцидент и опубликовала 700 ГБ информации, якобы украденной у Swisspro.

Кибератака на Le Slip Français

Производственный сектор
Утечка персональных данных

Французская компания Le Slip Français, производящая нижнее белье и домашнюю одежду, сообщила на своем сайте о том, что 15 апреля она подверглась кибератаке, в результате которой были скомпрометированы личные данные клиентов. По факту неавторизованного доступа к автоматизированной системе обработки данных была подана жалоба, а также направлен отчет во Французское управление по защите данных и другие органы правосудия. Компания уточнила, что инцидент затрагивает имена, фамилии, номера телефонов, почтовые адреса, адреса электронной почты, а иногда и номера заказов. Компания сообщила RTL, что часть данных учетных записей клиентов была украдена и опубликована в даркнете. Ответственность за утечку данных взял на себя злоумышленник под ником ShopifyGUY.

Кибератака на Lemken

Производственный сектор
Отказ ИТ-систем, отказ сервисов и нарушение операционной деятельности

Немецкий производитель сельскохозяйственной техники Lemken 11 мая подвергся кибератаке. Проникновение в сети компании имело глобальный масштаб и вызвало сбои в производстве и удаленной работе сотрудников. Атака затронула, в частности, обработку заказов на запасные части. Обнаружив нарушение безопасности, компания немедленно отключила свои ИТ-системы по всему миру, собрала группу реагирования с участием внешних экспертов и при содействии Государственного управления уголовной полиции. Согласно результатам первоначального анализа, данные клиентов не пострадали благодаря эффективным системам безопасности.

По словам генерального директора Lemken, работу некоторых из отключенных систем планировалось возобновить в течение нескольких дней. В июне компания возобновила производство машин на заводе в Альпене. Система электронной почты находилась под внешним управлением и не пострадала от атаки.

Кибератака на Crown Equipment

Производственный сектор
Утечка персональных данных, отказ в обслуживании и нарушение операционной деятельности

Американский производитель вилочных погрузчиков Crown Equipment признал, что подвергся кибератаке, которая привела к остановкам производства. Об этом свидетельствует письмо, полученное сотрудниками компании и 18 июня опубликованное сайтом BleepingComputer. С 10 июня производство на заводах компании в Родинге (Германия) и Нью-Бремене (США) было остановлено, до производителя нельзя было дозвониться, а сайт компании не работал. Расследование показало, что хакерам из международной группы удалось проникнуть в систему компании из-за того, что один из сотрудников предоставил несанкционированный доступ к своему устройству. Сотрудников предупредили, чтобы они не подтверждали запросы системы многофакторной аутентификации и проявляли бдительность в случае фишинга.

Позднее Crown Equipment сделала новое заявление, в котором подтвердила, что третья сторона получила неавторизованный доступ к некоторым данным компании, таким как отчеты о несчастных случаях и травмах, а также об участии сотрудников в льготных и пенсионных программах компании. В этих записях содержались конфиденциальные личные данные сотрудников, а в некоторых случаях еще и членов их семей.

Кибератака на LivaNova

Производственный сектор, медицина
Утечка персональных данных, отказ ИТ-систем

Британская компания LivaNova, производящая медицинское оборудование, уведомила около 130 тыс. человек о том, что их персональные данные были скомпрометированы в результате кибератаки в конце октября 2023 года. Согласно официальному письму, направленному пострадавшим, компания узнала об инциденте в середине ноября 2023 года. В ходе расследования выяснилось, что злоумышленники похитили в числе прочего имена, адреса, номера социального страхования и медицинскую информацию, а именно — диагноз, состояние, ход лечения, рецепты, имя врача, номер медицинской карты, серийный номер устройства и данные о медицинском страховании. Инцидент нарушил работу части ИТ-систем. Сразу после обнаружения проблемы компания начала расследование с привлечением внешних экспертов по кибербезопасности, координируя свои действия

с правоохранительными органами, и перевела некоторые системы в автономный режим. LivaNova сообщила об инциденте в конце апреля, вскоре после того, как были установлены его масштабы.

Кибератака на Taiwan United Renewable Energy

Производственный сектор, возобновляемая энергетика
Отказ ИТ-систем и нарушение операционной деятельности

Тайваньский производитель систем возобновляемой энергетики United Renewable Energy Co., Ltd. 11 апреля сообщил, что из-за кибератаки на некоторые ИТ-системы работа завода приостановлена и производится оценка финансовых последствий инцидента. ИТ-отдел компании принял необходимые защитные меры и начал операции по восстановлению совместно с внешними специалистами по обеспечению безопасности финансовой информации. На момент публикации сообщения все домены и связанные с ними файлы были тщательным образом отсканированы и проверены. После получения гарантий достаточного уровня информационной безопасности стали возможными восстановление данных из ежедневных резервных копий и возобновление работы.

Электронная промышленность

Утечка данных из Dell

Производственный сектор
Утечка персональных данных

Американский производитель и продавец компьютеров Dell 8 мая уведомил клиентов об утечке данных. В электронном письме компания сообщила, что расследует инцидент с порталом Dell, где хранится база данных с некоторой информацией о клиентах и совершенных ими покупках. Она включает имена, адреса, данные об оборудовании Dell и заказах на портале, сервисные коды, описание товаров, даты заказов и гарантийную информацию. Компания не сообщила, был ли инцидент связан с действиями сторонних злоумышленников или же со случайной ошибкой. 29 апреля сайт Daily Dark Web сообщил, что на одном из хакерских форумов некий злоумышленник предлагает информацию о покупках продуктов в Dell в период с 2017 по 2024 год, в том числе информацию о заказчиках. Если верить объявлению, в наборе данных содержится информация о 49 млн человек, включая полное имя, адрес, сервисный код системы, номер клиента и многое другое.

Злоумышленник, называющий себя Menelik, рассказал сайту TechCrunch, что для взлома портала Dell он подал заявку на регистрацию двух поддельных компаний в качестве партнеров (реселлеров продукции) Dell.

После одобрения заявки он вошел на портал и методом подбора получил доступ к сервисным кодам — они состояли лишь из семи символов и включали только цифры и согласные буквы. В процессе взаимодействия с клиентским порталом он выполнял по пять тысяч запросов в минуту в течение почти трех недель и при этом остался незамеченным компанией Dell.

Кибератака на BECOM

Производственный сектор, электронная промышленность, инженерная деятельность
Отказ в обслуживании, нарушение операционной деятельности

Австрийская компания BECOM, специализирующаяся на разработке, производстве и обслуживании электронной техники, 23 апреля подверглась кибератаке. Руководство компании заявило, что компания оперативно отреагировала на инцидент и отключила связь с интернетом, предотвратив тем самым шифрование данных. Первоочередной задачей было снова обеспечить работу производственных площадок. Компания сообщила, что прилагает все усилия, чтобы ускорить восстановление работы производственных площадок на объектах, и привлекает для этого внешних специалистов. Эти специалисты вместе с ИТ-отделом BECOM определили масштабы взлома, удалили вредоносное ПО из систем компании и проследили за тем, чтобы не осталось угроз, которые могли бы быть использованы в будущем. Компания проинформировала своих деловых партнеров о том, что обычные способы связи с ней были доступны лишь в ограниченном объеме.

Атака на корпорацию Key Tronic с применением шифровальщика

Производственный сектор, электронная промышленность
Утечка данных, утечка персональных данных, отказ в обслуживании, нарушение операционной деятельности
Шифровальщики

Американская корпорация Key Tronic (также известная как KeyTronic), занимающаяся производством электронной техники, 6 мая сообщила о киберинциденте в заявлении по форме 8-K, требуемом Комиссией по ценным бумагам и биржам. В ходе расследования и локализации атаки Key Tronic, следуя внутренним регламентам, привлекла внешних специалистов по кибербезопасности и уведомила власти об инциденте. Инцидент привел к нарушению работы и ограничению доступа к некоторым бизнес-приложениям компании, обеспечивающим различные аспекты ее деятельности и корпоративные функции, в том числе системы финансовой и операционной отчетности. Key Tronic считает, что несанкционированные действия были локализованы, и работает над восстановлением затронутых систем. На момент первоначального сообщения компания полагала, что инцидент не повлияет существенно на ее бизнес или финансовые результаты. 14 июня она обновила форму

и сообщила, что из-за атаки ей пришлось приостановить операции внутри страны и в Мексике на две недели. Однако в других регионах мира операции продолжались без нарушений, пока компания занималась устранением последствий атаки. После этого нормальная работа была возобновлена. В новом заявлении также говорится, что проведенное расследование подтвердило факт кражи персональных данных злоумышленниками. В соответствии с требованиями Комиссии по ценным бумагам и биржам, компания также подтвердила, что атака и потери продукции окажут существенное влияние на ее финансовое состояние в четвертом квартале, заканчивающемся 29 июня 2024 года.

В конце мая группа Black Basta взяла на себя ответственность за атаку, в результате которой было похищено 530 ГБ данных, включая финансовую и корпоративную информацию, инженерную документацию, а также персональные данные клиентов и сотрудников.

В более позднем заявлении компания оценила общие потери от инцидента в 17 млн долларов, указав, что «понесла около 2,3 млн долларов дополнительных расходов и потеряла примерно 15 млн долларов выручки в четвертом квартале».

Атака на Nexperia с применением шифровальщика

Производственный сектор, электронная промышленность
Утечка данных
Шифровальщики

Голландская компания Nexperia, принадлежащая китайскому владельцу и производящая полупроводниковые изделия, признала, что ее ИТ-системы подверглись взлому в марте 2024 года. Nexperia отключила затронутое оборудование для локализации бреши и начала расследование с привлечением внешних специалистов, чтобы определить характер и масштабы инцидента. Также компания приняла меры для предотвращения дальнейшего несанкционированного доступа и уведомила об инциденте соответствующие органы. Сообщение Nexperia об инциденте вышло после публикации 10 апреля данных вымогательской группой Dunghill Leak на одном из даркнет-сайтов. Хакеры утверждали, что похитили сотни гигабайт конфиденциальных материалов, таких как коммерческие секреты, проекты микросхем, а также сотни папок с данными клиентов, в том числе SpaceX, Apple и Huawei. Список украденных файлов, опубликованный на сайте в даркнете как доказательство взлома, включает конфиденциальные документы, например фотографию паспорта одного из сотрудников, а также юридическую и техническую документацию.

Атака на GlobalWafers с применением шифровальщика

Производственный сектор, электронная промышленность
Отказ ИТ-систем, отказ сервисов и нарушение операционной деятельности
Шифровальщики

Тайваньский производитель кремниевых пластин для полупроводников GlobalWafers 13 июня сообщил о кибератаке, которая затронула некоторые его производственные линии. Компания израсходовала существующие запасы для выполнения заказов, поэтому в третьем квартале возможны задержки с поставками. Были начаты мероприятия по расследованию и восстановлению данных, а также приняты меры по усилению кибербезопасности. Тщательное расследование подтвердило, что злоумышленники не смогли получить доступ к важной информации. В начальной фазе атак GlobalWafers частично отключила свои операционные системы, что повлияло на процессы производства и отгрузки на некоторых заводах. Компания заявила, что в будущем продолжит совершенствовать управление безопасностью сетевой и информационной инфраструктуры. 18 июня процессы отгрузки были частично восстановлены и в целом вернулись в нормальный режим. Вымогательская группа Black Basta включила компанию в список своих жертв.

Автомобильная отрасль

Кибератака на Sandhar Technologies

Производственный сектор, автомобилестроение
Отказ ИТ-систем

Индийская компания Sandhar Technologies, производящая автомобильные компоненты, 19 июня объявила об обнаружении инцидента безопасности, затронувшего несколько ее систем. Компания незамедлительно отреагировала на инцидент, мобилизовав свои технические подразделения и службы кибербезопасности для устранения угрозы. Компания заверила, что утечки конфиденциальных данных не произошло и инцидент не оказал существенного влияния на ее деятельность. 21 июня Sandhar Technologies выпустила новое заявление, в котором сообщила, что проблема успешно решена. Все финансовые, кадровые и конфиденциальные данные компании были сохранены и защищены благодаря ее партнеру в сфере облачных технологий. После инцидента все затронутые системы были успешно отформатированы и восстановлены. В ходе этого инцидента утечки конфиденциальных данных не произошло, ведь атака никак не затронула поставщика облачных услуг.

Кибератака на Meiller Kipper

Производственный сектор, автомобилестроение
Отказ ИТ-сервисов

Немецкий автопроизводитель Meiller Kipper подвергся кибератаке, из-за которой возникли ограничения в работе сотрудников и некоторых сервисов. Индикаторы компрометации передали компании власти, и Meiller Kipper привлекла специалистов по безопасности и криминалистов для оценки ситуации. В качестве меры предосторожности компания отключила все интернет-каналы связи, включая стационарные телефоны, чтобы защитить своих деловых партнеров, до завершения расследования. В связи с возникшими техническими ограничениями компания обратилась к поставщикам на своем сайте с просьбой повторно выставить счета до 10 июля.

Атака на CDK Global с применением шифровальщика

Автомобилестроение
Отказ ИТ-систем и нарушение операционной деятельности
Шифровальщики

Американская компания CDK Global, поставляющая решения по модели «программное обеспечение как услуга» для автомобильной промышленности, столкнулась с инцидентом безопасности, который нарушил работу североамериканских автосалонов и производителей автомобильного оборудования. CDK Global подверглась первой атаке 18 июня, после чего отключила системы из предосторожности. Некоторые сервисы были восстановлены 19 июня, но вечером произошла повторная атака, и системы снова отключили. Компания начала расследование с привлечением сторонних экспертов и уведомила об инциденте клиентов и правоохранительные органы. CDK Global организовала интерактивные линии голосовых ответов для информирования клиентов об атаке. По словам неназванных источников Bloomberg, CDK Global подверглась атаке с применением шифровальщика и договорилась о выплате выкупа группе BlackSuit. Компания предупредила своих клиентов о попытках фишинга со стороны мошенников, которые выдают себя за ее сотрудников, чтобы получить доступ к системе. По сообщению CBS News, 22 июня CDK Global разослала клиентам уведомление о том, что процесс восстановления займет несколько дней, и впервые охарактеризовала инцидент как «кибервымогательство».

В результате атаки была приостановлена работа около 15 000 автодилерских центров в США и Канаде, так как компания предоставляет программное обеспечение для управления ежедневными операциями, включая продажи, финансирование, страхование и ремонт автомобилей. Эта атака привела к серьезным сбоям в работе почти всех автодилеров, использующих сервисы CDK Global для ведения бизнеса.

По оценкам Anderson Economic Group, в результате этой кибератаки общие прямые убытки франчайзинговых дилерских центров могли составить 1,02 млрд долларов. Это потерянные доходы от продажи 56 200 новых автомобилей, а также запчастей, от предоставления услуг, дополнительные расходы на персонал, ИТ-среду и выплаты процентов по кредитам на товарные запасы за три календарные недели.

Пищевая промышленность

Атака на Lewis Brothers Bakeries с применением шифровальщика

Производственный сектор, пищевая промышленность
Утечка данных, утечка персональных данных, отказ ИТ-систем
Шифровальщики

Американский производитель продуктов питания Lewis Brothers Bakeries Inc. (LBBI) разослал 9 мая уведомление об утечке данных, которая произошла 1 апреля, когда злоумышленники зашифровали некоторые файлы на серверах компании. LBBI немедленно начала расследование характера и масштабов инцидента с привлечением сторонних специалистов по криминалистике. В ходе расследования было установлено, что в период с 25 марта по 1 апреля был осуществлен несанкционированный доступ к сети LBBI и из нее были скопированы и похищены определенные файлы. Компания провела всесторонний анализ данных, к которым потенциально мог быть получен несанкционированный доступ, чтобы определить, какого типа информация была затронута и к кому она относится. Согласно жалобе, поданной 17 мая в окружной суд США по Южному округу штата Индиана, среди утекших данных были имена, номера социального страхования и, возможно, другие сведения. LBBI уведомила об инциденте федеральные правоохранительные органы. Она также внедрила дополнительные меры безопасности и провела обучение сотрудников. 30 апреля группа Medusa взяла на себя ответственность за атаку.

Кибератака на Agropur

Производственный сектор, пищевая промышленность
Утечка данных

Канадский производитель молочных продуктов Agropur стал жертвой кибератаки, затронувшей часть его онлайн-каталога. Компания заявила, что ее деятельность не была нарушена и что были приняты меры по устранению последствий инцидента и усилению защиты данных. Agropur заявила, что взлом не затронул ее транзакционные системы. В своем уведомительном письме компания отметила, что нет никаких доказательств несанкционированного использования затронутых данных, но из соображений осторожности она предупредила клиентов о возможных

рисках, пока расследование не завершится и не станет доступна более подробная информация. Компания начала расследование, чтобы определить масштабы и последствия для клиентов, и обратилась за помощью к внешним экспертам по кибербезопасности и правоохранительным органам.

Строительство

Кибератака на Eucatex

Производственный сектор, строительство
Отказ ИТ-сервисов
Шифровальщики

Бразильский производитель строительных материалов и мебели для дома Eucatex 2 мая сообщил, что подвергся кибератаке, которая привела к остановке его ERP-системы и электронной почты. В компании заверили, что базы данных остались в сохранности и не было обнаружено никаких признаков потери или утечки информации. Проблема была решена, и системы были восстановлены. Компания сообщила, что будет информировать финансовый рынок и компетентные органы о появлении новых сведений.

Вымогательская группа RansomHub добавила Eucatex в список своих жертв. Злоумышленники заявили, что похитили 150 ГБ конфиденциальной информации, включая данные о клиентах и подрядчиках, финансовые документы, соглашения о неразглашении и исходные коды приложений.

Кибератака на Wehrle-Werk

Строительство, инженерная деятельность
Отказ в обслуживании и нарушение операционной деятельности

Немецкая машиностроительная и строительная компания Wehrle-Werk подверглась кибератаке. По данным SentiGuard, она произошла 11 мая. С этого момента производство и коммуникации компании были сильно ограничены. 22 мая Wehrle-Werk объявила, что интенсивно работает над восстановлением пострадавших систем и возобновлением полноценной работы. Внутреннему ИТ-отделу компании помогает поставщик ИТ-услуг.

Атака на Max Wild с применением шифровальщика

Строительство, логистика
Утечка данных, отказ ИТ-систем, отказ ИТ-сервисов
Шифровальщики

Немецкая логистическая и строительная компания Max Wild GmbH стала жертвой кибератаки, которая была обнаружена 25 апреля и немедленно остановлена. По сообщению на сайте компании, в ходе атаки злоумышленникам удалось преодолеть барьеры ИТ-безопасности и существующие системы защиты и проникнуть в ИТ-системы. В результате многие ИТ-системы компании были отключены, в частности сервисы для коммуникации, планирования встреч и электронная почта. Компания попросила при возникновении срочных вопросов пользоваться телефоном.

С помощью внешних и внутренних специалистов Max Wild GmbH зафиксировала следы кибератаки и детально изучила ее последствия для своих ИТ-систем. Ответственность за атаку взяла на себя вымогательская группа MetaEncryptor. По ее утверждению, было похищено 85 ГБ данных.

Фармацевтическая отрасль

Атака на Octapharma Plasma с применением шифровальщика

Производственный сектор, фармацевтика
Утечка данных, утечка персональных данных, отказ ИТ-систем, нарушение операционной деятельности
Шифровальщики

Швейцарская медицинская и фармацевтическая компания Octapharma 17 апреля обнаружила несанкционированную сетевую активность, которая привела к временному закрытию более 150 центров донорства плазмы в США. Согласно сообщениям на сайте компании, центры донорства плазмы в Германии не пострадали и продолжали работу в обычном режиме, работа европейских производственных площадок продолжалась в нормальном режиме. Для расследования атаки компания инициировала процедуры реагирования на инциденты, а также перевела системы в автономный режим, чтобы ограничить возможные последствия инцидента.

Ответственность за атаку взяла на себя вымогательская группа BlackSuit, которая заявила, что похитила данные о бизнесе, а также лабораторные и персональные сведения. Источник сообщил изданию The Register, что вымогательская группа проникла в компанию через системы VMware и что перебои в работе в США могут повлиять на поставки плазмы в европейские подразделения Octapharma. Расследование взлома, проведенное при помощи сторонних экспертов по кибербезопасности и ФБР, завершилось 2 августа. Octapharma сообщила, что были скомпрометированы данные из ее файлообменных систем,

что потенциально могло затронуть личную информацию клиентов. Среди затронутых данных такие конфиденциальные сведения, как полные имена, номера социального страхования, номера водительских прав, номера финансовых счетов, информация о медицинском страховании.
Было определено, что от инцидента могли пострадать около 1423 жителей. Пострадавшие были уведомлены об инциденте. В качестве компенсации им была предложена услуга по кредитному мониторингу бесплатно в течение двух лет. Эта услуга предполагает не только защиту личных данных от кражи, но и отслеживание кредитной активности клиентов для предотвращения мошеннических действий с кредитными картами или займами.

Кибератака на Rekah

Производственный сектор, фармацевтика
Отказ ИТ-систем, нарушение поставок продукции

Крупная израильская фармацевтическая компания Rekah, производящая лекарства, косметику, витамины и пищевые добавки, подверглась кибератаке и отключила свою систему дистрибуции, что было подтверждено Calcalistech. Компания провела работы по локализации инцидента и отражению атаки, а также восстановлению скомпрометированных систем. Согласно заявлению Rekah для фондовой биржи от 17 июня, компания выявила потенциальный инцидент кибербезопасности, связанный с несанкционированным проникновением третьей стороны в компьютерные системы дочерней компании Ophir & Shalpharm Medicines and Cosmetics, которая полностью управляет центральной системой дистрибуции и продаж компании Rekah. По словам исполнительного директора Rekah, компания прикладывает усилия для того, чтобы как можно быстрее восстановить систему дистрибуции, и одновременно тестирует ручные методы управления на случай, если расследование затянется. Была создана специальная команда, в которую также вошли сторонние специалисты. По оценкам топ-менеджера, кратковременная остановка системы дистрибуции не приведет к дефициту лекарств, выпускаемых компанией. Производственная система Rekah не пострадала и продолжила функционировать в обычном режиме.

Кибератака на Pharmascience

Производственный сектор, фармацевтика
Нарушение операционной деятельности

Канадский производитель фармацевтических препаратов Pharmascience стал жертвой кибератаки, по сообщениям местных СМИ. Компания подтвердила, что обнаружила вторжение в свою компьютерную систему 1 июня, но не сообщила подробности о масштабах и продолжительности атаки. Она также не уточнила, был ли запрошен или выплачен выкуп и были ли похищены данные. Компания быстро привлекла специалистов по кибербезопасности для защиты своих систем. По информации из электронного письма компании, она возобновила работу в безопасном и эффективном режиме.

Горнодобывающая промышленность и металлургия

Атака на Westfälische Stahlgesellschaf с применением шифровальщика

Производственный сектор, металлургия
Утечка данных, утечка персональных данных, отказ ИТ-систем
Шифровальщики

Немецкая сталелитейная компания Westfälische Stahlgesellschaf стала жертвой атаки с использованием шифровальщика, говорится в сообщении на ее сайте. 9 июня злоумышленники скачали из систем компании некоторые данные и зашифровали данные на системах организации. Инцидент не повлиял на производство, и компания уверена, что сможет выполнить все поставки в срок. Однако инцидент затронул персональные данные сотрудников. Westfälische Stahlgesellschaf немедленно закрыла доступ к своим ИТ-системам через интернет, восстановила системы и данные из резервных копий и уведомила об инциденте органы по надзору за защитой данных. Ответственность за атаку взяла на себя вымогательская группа LockBit 3.0.

Атака на Schuette с применением шифровальщика

Производственный сектор, металлургия
Утечка данных, утечка персональных данных
Шифровальщики

Американская компания по производству металла Schuette Inc. сообщила о том, что стала жертвой атаки с использованием шифровальщика. Согласно заявлению компании, 18 апреля Schuette стало известно о несанкционированной активности в ее компьютерных системах. После обнаружения инцидента компания немедленно обеспечила защиту сети и оперативно привлекла внешнюю команду криминалистов, чтобы определить характер и масштаб инцидента. К 14 мая после тщательного расследования Schuette выяснила, что третья сторона могла получить несанкционированный доступ к некоторым персональным данным. Компания заявила, что нет доказательств несанкционированного использования какой-либо информации. Она также отметила, что данные, к которым получили доступ злоумышленники, могли включать имя, фамилию и номер социального страхования. 28 мая 2024 года Schuette начала уведомлять людей, чьи данные могли быть затронуты.

Узнав об инциденте примерно через месяц после произошедшего, компания предприняла меры по защите своих систем и усилению безопасности сети, чтобы предотвратить подобные инциденты в будущем. 20 мая вымогательская группа Cactus добавила компанию Schuette Metals в список своих жертв.

Атака на Northern Minerals с применением шифровальщика

Горнодобывающая промышленность
Утечка данных, утечка персональных данных
Шифровальщики

Австралийская компания Northern Minerals, занимающаяся добычей редкоземельных металлов, 4 июня сообщила о компрометации некоторых своих данных, которые оказались в даркнете в результате кибератаки, произошедшей в конце марта 2024 года. Согласно заявлению компании, взлом не оказал существенного влияния на ее деятельность. Компания проанализировала свои рабочие процессы, приняла меры по укреплению защиты своих систем, уведомила об инциденте соответствующие органы и воспользовалась помощью специалистов по юридическим, техническим и вопросам кибербезопасности. Это заявление было сделано вскоре после того, как вымогательская группа BianLian опубликовала на своем Tor-сайте утечек несколько архивов, предположительно содержащих рабочие, кадровые, управленческие, проектные данные, а также данные электронных писем, похищенные у Northern Minerals. Утечка данных затронула корпоративную, операционную и финансовую информацию, а также данные о нынешних и бывших сотрудниках и сведения об акционерах, сообщила компания Northern Minerals.

Министерство иностранных дел и торговли подтвердило, что личные данные некоторых нынешних и бывших работников Northern Minerals были скомпрометированы. Ведомство также сообщило, что скомпрометированные австралийские паспорта по-прежнему можно использовать для международных поездок.

Кибератака на Iluka Resources

Горнодобывающая промышленность
Отказ в обслуживании

Австралийская горнодобывающая компания и поставщик редкоземельных металлов Iluka Resources сообщила, что злоумышленники пытались нарушить работу ее внешнего сайта посредством DoS-атаки, но им не удалось получить доступ к системам компании или похитить какие-либо данные. После запросов со стороны местных СМИ представитель компании подтвердил, что она столкнулась с инцидентом безопасности, о котором сообщила властям.

Логистика и транспорт

Кибератака на Barnett's Couriers

Логистика
Отказ в обслуживании, нарушение операционной деятельности

Австралийская логистическая компания Barnett's Couriers стала жертвой кибератаки, что привело к закрытию бизнеса, сообщается в уведомлении, которое воспроизводится при звонке на телефон горячей линии. В результате атаки была нарушена полноценная работа компании. «Вместе с ведущими ИТ-консультантами Barnett's Couriers неустанно работала над восстановлением своих систем, но, к сожалению, не смогла справиться с трудностями и приняла непростое решение прекратить деятельность». В автоматических ответах по электронной почте, аналогично голосовым сообщениям, добавляется, что в компании работает небольшой коллектив, «который в ближайшие недели завершит обработку всех незакрытых счетов». Полиция Нового Южного Уэльса изначально заявила, что компания не сообщала о кибератаке, которая могла бы стать причиной внезапного закрытия предприятия. Сотрудники и водители получили уведомление о том, что с 1 мая они больше не работают в компании, за несколько часов до увольнения. В июне представитель полиции Нового Южного Уэльса подтвердил, что правоохранительные органы начали расследование кибератаки на Barnett's Couriers.

Атака на Skanlog с применением шифровальщика

Логистика
Отказ ИТ-систем и нарушение операционной деятельности
Шифровальщики

Датская логистическая компания Skanlog подверглась атаке с использованием шифровальщика, сообщил топ-менеджер компании шведским СМИ. В результате атаки вся система была отключена до тех пор, пока ее не удалось восстановить и вернуть в эксплуатацию. Атака может повлиять на поставки товаров в сети магазинов, основным подрядчиком которых является Skanlog.

Атака на порт Сан-Франсиску-ду-Сул с применением шифровальщика

Транспорт, логистика, порты
Утечка данных, отказ ИТ-систем, нарушение операционной деятельности
Шифровальщики

Порт Сан-Франсиску-ду-Сул в Бразилии опубликовал официальное сообщение, в котором говорится, что 6 мая на его сервер была совершена кибератака, в результате чего были зашифрованы некоторые данные. Чтобы предотвратить распространение атаки, системы были временно отключены. 7 мая ИТ-команде порта благодаря поддержке поставщиков услуг удалось частично восстановить работоспособность системы. Это позволило полностью возобновить работу порта менее чем за сутки. Порт сообщил, что изучает объем затронутых атакой данных. Постепенно восстанавливаются системы контроля доступа и безопасности, в частности автоматическое считывание номерных знаков, биометрия и видеонаблюдение. Об атаке было сообщено в Федеральную налоговую службу, которая разрешила порту возобновить работу, в Национальное агентство водного транспорта и Национальное управление по защите данных. Вымогательская группа RansomHub взяла на себя ответственность за атаку на порт Сан-Франсиску-ду-Сул, заявив, что было похищено 548,72 ГБ данных, включая бухгалтерские данные, финансовые отчеты и данные о сотрудниках.

Атака на Ocasa с применением шифровальщика

Логистика
Отказ ИТ-систем и нарушение операционной деятельности
Шифровальщики

Аргентинская логистическая компания Ocasa подверглась атаке с использованием шифровальщика, в результате чего перестал работать сайт компании и были нарушены ее рабочие процессы, что подтвердили местные СМИ. Компания предприняла действия по локализации утечки, восстановлению работы сервисов и защите своих систем, одновременно выясняя масштабы ущерба. На момент поступления официального подтверждения атаки от компании ее сайт все еще не работал, однако представители Ocasa заявляли, что утечки данных не было.

Атака затронула и другие компании из группы, управляющей Ocasa, в частности Direxa. Это компания, предлагающая индивидуальные и эксклюзивные решения в области комплексных логистических услуг, импорта, экспорта и транзитных операций с товарами. 26 июня вымогательская группа Akira добавила информацию об Ocasa на свой даркнет-портал.

Коммунальные службы

Кибератака на Tipton Municipal Utilities

Водоснабжение, энергоснабжение, коммунальные службы
Нарушение операционной деятельности

Американская компания Tipton Municipal Utilities (TMU), обеспечивающая электроснабжение, водоснабжение и очистку сточных вод в городе Типтоне, подверглась кибератаке. 20 апреля Народная киберармия России разместила в Telegram видеоролик, в котором заявила о своей причастности к кибератаке на водоочистные станции TMU. На видео, опубликованном хакерами, показано, как они якобы управляют программным обеспечением, которое контролирует оборудование для аэрации и перемещения жидкостей на водоочистных станциях в Типтоне. Генеральный директор TMU сообщил CNN, что они стали объектом атаки, но компрометации не произошло. По его словам, перебои в работе TMU были минимальными, и компания продолжала работать все время. Федеральные власти провели расследование инцидента. Согласно комментарию генерального директора TMU изданию StateScoop, кибератака начала отражаться на работе компании в Типтоне вечером 19 апреля. Руководство завода отправило сотрудников на устранение неполадок, которые снова прервали работу компании утром 21 апреля. Он назвал перебои в работе станции незначительными и сказал, что они никак не сказались бы на снабжении города питьевой водой. TMU сохраняла работоспособность станции на протяжении всего инцидента и продолжала принимать и очищать сточные воды даже во время перебоев.

Атака на Emcali с применением шифровальщика

Водоснабжение, энергоснабжение, коммунальные службы
Отказ ИТ-систем
Шифровальщики

Колумбийская коммунальная компания Emcali подверглась серьезной кибератаке, в ходе которой злоумышленники хотели вывести из строя бизнес и биллинговые системы. Атака, начавшаяся 9 июня, была локализована менее чем за два часа благодаря оперативному реагированию внутренней службы безопасности. Сначала атака затронула веб-сайт компании. Управляющий Emcali сообщил местным СМИ, что атака, очевидно, была направлена на информационные системы, связанные с коммерческой деятельностью. Компании пришлось изолировать свои системы и заново их подключать и включать. Начато расследование для определения исполнителей атаки и их мотивов. По мнению представителей Emcali, злоумышленники действовали с целью вымогательства или саботажа.

Кибератака на Sawnee EMC

Энергетика, коммунальные службы
Отказ ИТ-сервисов

Американская энергоснабжающая компания Sawnee Electric Membership Corporation 6 мая сообщила клиентам по электронной почте, что ее сайт был взломан в результате киберинцидента. Клиентам рекомендовали не пытаться зайти на старый сайт sawnee[.]com и не открывать никакие ссылки на нем, а использовать новый сайт www.sawnee[.]coop. Компания заявила, что в настоящее время проводится всестороннее расследование произошедшего инцидента безопасности.

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky ICS CERT) — глобальный проект «Лаборатории Касперского», нацеленный на координацию действий производителей систем автоматизации, владельцев и операторов промышленных объектов, исследователей информационной безопасности при решении задач защиты промышленных предприятий и объектов критически важных инфраструктур.

Kaspersky ICS CERT ics-cert@kaspersky.com