Последствия ransomware: от убытков на миллионы до закрытия

В результате недавнего киберинцидента, который предположительно был ransomware-атакой, Demant, один из крупнейших в мире производителей слуховых аппаратов, ожидает убытки на сумму до 95 миллионов долларов.

По всей видимости, ущерб Demant из-за вируса-вымогателя будет крупнейшим со времен эпидемии шифровальщика NotPetya, когда ведущие компании, такие как морской перевозчик Maersk и служба курьерской доставки FedEx, потеряли более 300 миллионов долларов каждая.

Предполагаемые убытки Demant выше, чем у Norsk Hydro, который тоже недавно стал жертвой кибервымогателей. Первоначально ущерб от ransomware-атаки у норвежского производителя алюминия оценивался в 40 миллионов долларов, но последние подсчеты показывают, что общая сумма достигнет 70 миллионов долларов.

Что именно произошло у Demant, вряд ли станет известно широкой общественности, поскольку компания крайне скупа на информацию. 3 сентября датский вендор лишь объявил, что из-за "критического инцидента", связанного с атакой киберпреступников, он отключает всю свою внутреннюю ИТ-инфраструктуру.

Судя по публикациям в датских СМИ, которые изучили обозреватели ZDNet, ИТ-сеть Demant атаковал вирус-шифровальщик. Косвенно это подтверждается в пресс-релизе Demant от 26 сентября, в котором рассказывается о финансовых последствиях киберинцидента. В тексте говорится, что благодаря оперативной реакции резервные копии данных в целом не пострадали, и компания использует их для восстановления.

Маловероятно, что случившееся было утечкой данных, поскольку после таких инцидентов компании обычно приходят в себя уже через несколько дней. Demant до сих пор восстанавливается и предупредила, что для завершения процесса нужно еще две-три недели. Длительное восстановление ИТ-инфраструктуры характерно как раз при устранении последствий ransomware-атак.

Очевидно, что Demant сильно пострадала. По данным компании, инцидент затронул ее ERP-систему, производственные, сбытовые и сервисные центры в Польше, Мексике, Франции и Дании, а также всю ИТ-сеть в Азиатско-Тихоокеанском регионе.

Помимо непосредственного ущерба ИТ-инфраструктуре, значительные убытки Demant понесла из-за недоступности систем, что привело к задержкам поставок продукции и проблемам с размещением заказов. Также инцидент нарушил регулярное обслуживание пациентов в клиниках, входящих в клиентскую сеть датского вендора.

Все это обернулось финансовой катастрофой для Demant. Компания предупредила, что общие убытки, предположительно, будут варьироваться в диапазоне от 550 до 650 миллионов датских крон. В пересчете на американскую валюту это составляет 80-95 миллионов долларов. Страховка на случай киберинцидента покроет лишь незначительную часть этой суммы - порядка 14,6 миллиона долларов.

Основные потери компания понесла из-за упущенных продаж и невозможности выполнить заказы. Что касается непосредственного ущерба ИТ-инфраструктуре, то затраты на ее восстановление оцениваются примерно в 7,3 миллиона долларов. Считай, капля в море, если сравнивать с общей суммой.

> "Это киберпреступление существенно повлияло на нашу способность к росту, на который мы рассчитывали во втором полугодии. Хотя коммерческий отдел предпринимает все возможное, чтобы компенсировать последствия инцидента, ситуация такова, что мы не сможем в полной мере реализовать наши амбициозные коммерческие планы. Мы работаем круглые сутки, чтобы вернуться к прежнему, ориентированному на рост бизнеса курсу, параллельно минимизируя негативные последствия для клиентов и пользователей нашей продукции", - заявил президент и генеральный директор Demant Сорен Нильсен (Soren Nielsen).

Наряду с Demant от кибератаки недавно пострадал и немецкий производитель военной техники и вооружения Rheinmetall. 26 сентября в пресс-службе Rheinmetall предупредили о сбоях в работе заводов в Бразилии, Мексики и США из-за распространения вредоносного ПО.

Среди других крупных компаний, которые пали жертвами вирусов-шифровальщиков за последнее время - производитель запчастей для авиационной техники ASCO, уже упомянутая Norsk Hydro, американские фирмы Hexion и Momentive, выпускающие смолы, силиконы и другие материалы, швейцарский производитель строительной и дорожной спецтехники Aebi Schmidt, американский поставщик напитков Arizona Beverages, французская инженерная компания Altran. Также в этом списке Международный аэропорт Кливленд, полицейская федерация Англии и Уэльса и даже компания Verint, специализирующаяся на информационной безопасности.

Последствия ransomware-атак на организации в каждом случае разные, и порой дело может дойти до закрытия. Так произошло с калифорнийской клиникой Wood Ranch Medical (WRM), сообщает издание HealthITSecurity.

В августе 2019 года вирус-вымогатель поразил серверы WRM, на которых находились данные пациентов клиники. Вместе с медицинскими картами зашифрованными оказались и резервные копии, хранившиеся на жестких дисках. Информация была настолько повреждена, что восстановить ее уже невозможно. В связи с этим руководство клиники объявило о ее полном закрытии и прекращении деятельности с 17 декабря 2019 года.

Wood Ranch Medical - уже вторая клиника в США за последний год, которая закрывается после ransomware-атаки. Ранее такая же участь постигла Бруксайдский центр слуха и оториноларингологии (Brookside ENT and Hearing Center) в Мичигане. Его компьютерные системы были полностью зашифрованы, а кибервымогатели потребовали 6500 долларов за дешифровку файлов. Однако клиника отказалась платить выкуп, после чего хакеры удалили все данные.