Крупнейшие скандалы с утечкой данных: от потерянных документов до вирусов-вымогателей

rus.db.lv, 14/03/2018, Rus.db.lv

В последние месяцы у всех на устах задачи, которые предстоят в связи с внедрением в жизнь Общего регламента о защите данных, или GDPR. Хотя многие сетуют на трудоемкость и дороговизну этого процесса, в долгосрочной перспективе выиграют и предприниматели, и частные лица, считает адвокат и партнер бюро присяжных адвокатов "Sorainen" Агрис Репшс.

По словам эксперта, внедрение GDPR (англ. General Data Protection Regulation), разумеется, не гарантирует, что в будущем мы не столкнемся с утечками данных и кибератаками, однако регламент вынуждает предпринимателей обращаться с данным более ответственно, а также пересмотреть процессы, связанные с управлением и хранением данных. В центре внимания общественности не раз оказывались скандалы о взломе систем и утечке данных, которых можно было бы избежать, если бы компании уделяли должное внимание защите обрабатываемых данных.

"При введении требований регламента одинаково большое значение имеют и юридические, и информационно-технологические процессы, поэтому "Sorainen" объединило усилия с ИТ-компанией "Squalio" и разработало совместную услугу "GDPR Ready, которая включает в себя независимый юридический аудит и аудит ИТ-систем, профессиональные рекомендации о необходимых изменениях, чтобы предприятие было готово к GDPR", - говорит А. Репшс.

"Uber" заплатил хакерам 80 000 евро

В 2016 году хакеры взломали базы данных "Uber" и получили доступ к именам, фамилиям, адресам электронной почты и номерам мобильных телефонов 57 миллионов клиентов, а также к персональным данным 600 тысяч водителей такси, включая информацию о лицензиях. Этот инцидент стал достоянием гласности только в 2017 году - оказывается, "Uber" заплатил хакерам 80 тысяч евро, чтобы похищенные данные были уничтожены и никогда не использовались.

"Фактически все эти люди могут стать жертвой различных кибератак - мошенничества через электронную почту, фишинга и даже похищения идентичности. "Uber" обеспечивает таксистам бесплатную защиту, чтобы от их имени не оформлялись мошенническим путем кредиты, но пострадавшим клиентам пока ничего не предложено", - отмечает представитель компании "Squalio" Марек Грушкевиц.

Литовская клиника пластической хирургии вымогателям не заплатила и оказалась в центре скандала

Весной 2017 года стало известно о том, что киберпреступники украли данные пациентов, их фотографии, в том числе в обнаженном виде и фото "до и после", из литовской клиники пластической хирургии "Grožio Chirurgija" и выставили их на продажу в "темном интернете" ("dark web"). Цены варьировались от 50 до 2000 евро за карточку пациента, а все вместе можно было приобрести за 300 биткойнов или примерно 344 тысячи евро. Среди пациентов клиники были как местные, так и международные знаменитости, которых эти киберпреступники шантажировали.

Хакеры опубликовали информацию о том, что вначале пытались шантажировать клинику, называя требуемый выкуп относительно небольшой платой за уязвимость ИТ-систем, которые это медицинское учреждение использует. "Клиника отказалась это сделать (кажется, у них очень, очень и очень большое ЭГО), поэтому мы создали этот сайт и предлагаем купить данные все желающим", - заявили хакеры. Ссылку на сайт с похищенными данными преступники отправили одному из крупнейших литовских СМИ "15min.lt". Более подробно об этом деле можно прочитать здесь.

Даже "Deloitte" стала жертвой кибератаки

К сожалению, даже одна из крупнейших в мире аудиторских фирм "Deloitte", а конкретнее, ее бюро в Нью-Йорке, пострадало в результате кибератаки, когда была взломана система ее корпоративной электронной почты, писала в сентябре прошлого года "The Guardian". Считается, что хакеры, вероятно, получили информацию о лучших клиентах компании ("blue-chips") - их фамилии, пароли, личные данные, конфиденциальную переписку. Среди пострадавших в основном были клиенты из США, но не исключено, что также клиенты из Великобритании.

"Компания обнаружила взлом в марте 2017 года, но считается, что хакеры получили доступ к системе еще осенью 2016 года. Эффективная ИТ-система позволяет заметить такие взломы гораздо раньше. Кроме того, если раньше предприятия сами могли решать, информировать или нет о происшествии, то теперь этого нельзя будет избежать, потому что GDPR предписывает сообщать о всех происшествиях в обязательном порядке", - поясняет Грушкевиц.

В Швеции из-за утечки конфиденциальных данных должностей лишились два министра

В августе прошлого года из-за утечки конфиденциальных данных в Швеции должностей лишились министр внутренних дел Андерс Игеман, министр инфраструктуры Анна Йохансон и руководитель Национального транспортного агентства (НТА) Мария Агрен, сообщала "The Guardian".

Как пишет издание, нарушение произошло в 2015 году, когда НТА наняло как поставщика аутсорсинговых услуг некую ИТ-компанию, но не провела проверку ее персонала. В результате произошла утечка национальной базы данных лицензий автоводителей, возможно, также информации о транспорте секретных служб, армии и полиции, а также данных о лицах, в отношении которых начаты уголовные дела, и людях, включенных в программу защиты свидетелей. Правда, НТА отрицало, что в его распоряжении была информация оборонного характера. Кроме того, до сих пор нет никаких сведений о том, что эти данные "были распространены в каком-либо ненадлежащем виде".

"2017 год иногда называют кибергеддоном, потому что компании и частные лица подвергались скандальным кибератакам, например, "WannaCry", "NotPetya" и др. Поэтому внедрение GDPR являетс

я логичным решением Европейского союза, а именно, на предпринимателей возложена обязанность заботиться о приватности и безопасности клиентов", - заключает А. Репшс. Он добавляет, что в то же время и сами люди должны стать более сознательными и осторожными, делясь своими данными и данными членов своей семьи.
rus.db.lv

http://rus.db.lv/ekonomika/tehnologii/krupnejshie-skandaly-s-utechkoj-dannyh-ot-poterjannyh-dokumentov-do-virusov-vymogatelej-85205