Кибератака затронула федеральные учреждения Швейцарии | Une cyberattaque touche les offices fédéraux suisses

Автор: Заррина Салимова, Берн , 06.06.2023.

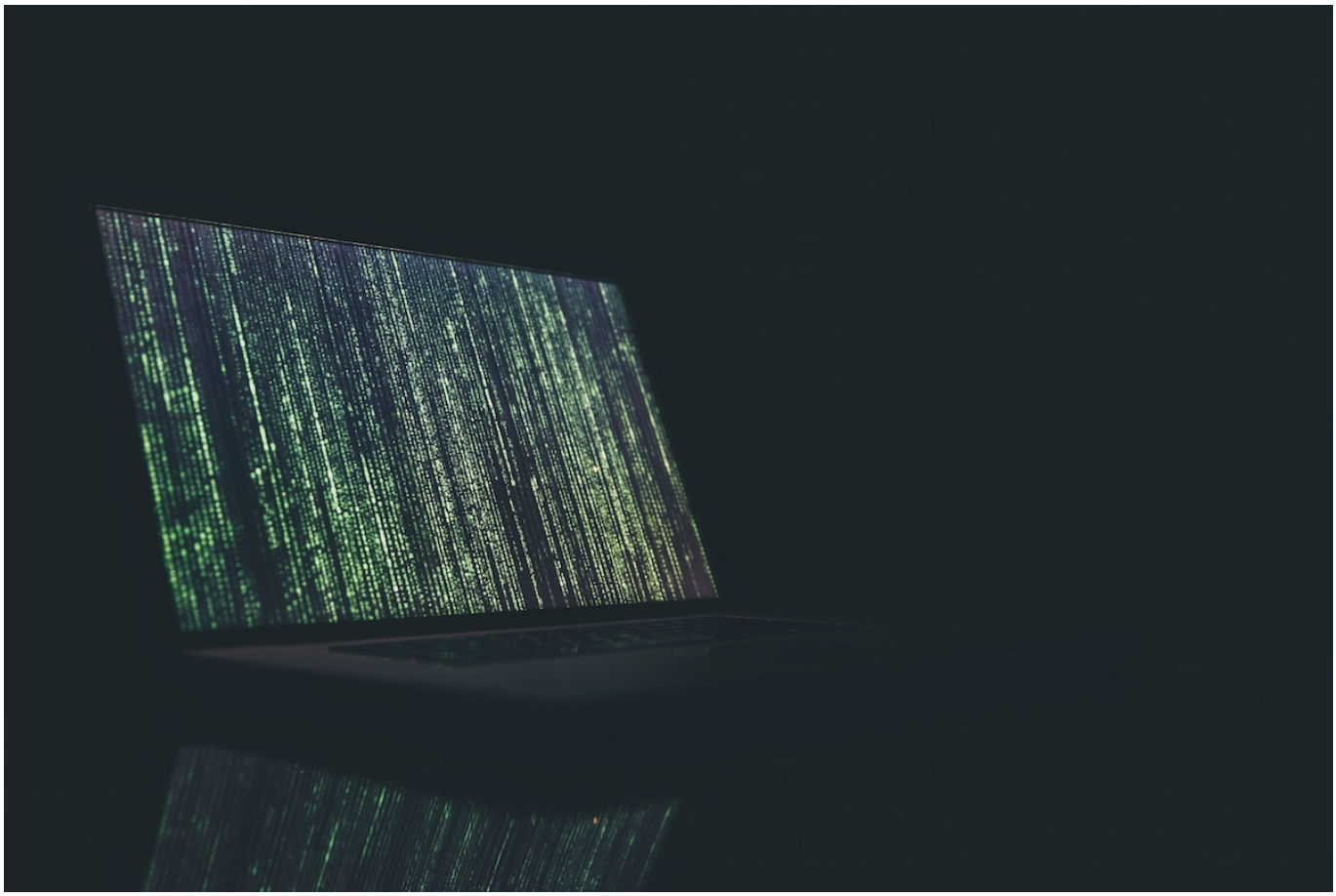

Фото: Markus Spiske, Unsplash

От действий хакеров косвенно пострадали армия, таможня и Федеральное управление полиции (Fedpol).

|

Le piratage informatique a touché indirectement l’armée, les douanes et Fedpol.

Une cyberattaque touche les offices fédéraux suisses

Жертвами киберпреступников в Швейцарии уже становились местные органы власти, включая расположенный в кантоне Во городок Ролль, врачебные кабинеты, университеты, СМИ и такие крупные компании, как ABB и Swissport. Но недавняя атака отличается от предыдущих, так как она впервые затронула государственные силовые структуры.

Первыми о беспрецедентном хакерском нападении сообщили журналисты Le Temps. По их информации, пострадали несколько кантональных полицейских управлений, швейцарская армия, таможня и Fedpol. Все эти учреждения объединяет то, что они пользовались услугами берснкой ИТ-компании Xplain, которая и стала первоначальной целью хакеров. Взлом – дело рук киберпреступников из группы Play, которые ранее уже атаковали медиахолдинги CH Media и NZZ, а также поставщика ИТ-услуг Unico Data и муниципалитет Саксона в кантоне Вале.

Поставщик программного обеспечения проинформировал об инциденте соответствующие структуры, отметив, что не хранит в своих системах никаких данных о частных лицах или бизнесе клиентов. На шантаж вымогателей фирма не поддалась, отказавшись от контактов с ними. «Мы не будем платить выкуп», - подчеркнул в комментарии Le Temps директор Xplain Андреас Лёвингер. Компания обратилась за помощью в Национальный центр кибербезопасности.

Киберпреступники угрожали опубликовать в даркнете в общей сложности 907 гигабайтов данных, если не будет заплачен выкуп, но пока обнародовали лишь часть данных. По оценкам Le Temps, речь идет о шести сжатых файлах с тысячами документов общим объемом около трех гигабайтов. В них содержится информация о многочисленных ИТ-проектах, реализованных Fedpol совместно с несколькими кантональными полицейскими управлениями: контракты, технические спецификации, идентификаторы для доступа к определенным услугам и прочее. В сети размещены и документы, имеющие отношение к таможне, Ruag Group, Rega и армии.

По имеющимся на данный момент сведениям, ни один проект Fedpol не пострадал, так как у Xplain есть анонимные данные для целей тестирования, но нет доступа к оперативным данным. Федеральное управление таможенной и пограничной охраны также подтвердило, что данные переписки с Xplain скомпрометированы, но собственные данные Управления не пострадали. По словам пресс-секретаря Федерального министерства обороны, на основании разъяснений, сделанных армией на сегодняшний день, инцидент не привел к утечке данных из армейских систем.

Таким образом, пока затронутые ведомства полагают, что данные из действующих проектов не были похищены. С этой точки зрения происшествие может показаться не очень серьезным. Но это не совсем так: кибератака продемонстрировала уязвимость сторонних технологических компаний, которые располагают конфиденциальной информацией и взлом которых может иметь серьезные последствия. Так, атака Unico Data парализовала часть ИТ-системы ее клиента Pathé, оператора кинотеатров. Такие фирмы – привлекательные цели для хакеров, которые могут разом похитить данные десятков или даже сотен клиентов. Эксперты сходятся во мнении, что поставщикам ИТ-услуг следует быть особенно осторожными, например, тщательно взвешивая плюсы и минусы размещения на сайте списка своих клиентов, что потенциально может привлечь внимание хакеров.

Добавим, что бдительность не стоит терять не только компаниям, но и обычным

пользователям. Национальный центр кибербезопасности, например, рекомендует постоянно пользоваться функцией многофакторной аутентификации, которая обеспечивает дополнительную защиту от несанкционированного доступа к системе или приложению: активируйте многофакторную аутентификацию для всех конфиденциальных учетных записей, включая электронную почту, интернет-банкинг и социальные сети, а также регулярно проверяйте настройки этой функции.

Швейцария
кибербезопасность
Статьи по теме
Бум киберпреступности в Швейцарии
Готова ли Швейцария к кибервойне?
Женева станет столицей мировой кибербезопасности?
В Швейцарии воруют в киберпространстве
Швейцария под прицелом хакеров
Швейцарцы также пострадали от хакеров Anonymous
