

Цена киберпреступности в Швейцарии и в мире | Le coût de la cybercriminalité en Suisse et dans le monde

Author: Лейла Бабаева, [Берн-Лозанна-Цюрих](#) , 13.05.2021.



© TheDigitalArtist/pixabay.com

На фоне пандемии число обычных преступлений в Швейцарии сократилось, но участились случаи правонарушений в интернете. Жертвами злоумышленников становятся как простые граждане, так и компании, некоторые из них закрываются из-за неспособности заплатить выкуп мошенникам, использующим программы-вымогатели.

Au milieu de la pandémie, le nombre de crimes de droit commun en Suisse a diminué, mais le nombre de crimes sur Internet a augmenté. Parmi les victimes de cybercriminels sont des individus et des entreprises, certaines d'entre elles font faillite en raison de leur incapacité à payer les rançon aux escrocs.

Le coût de la cybercriminalité en Suisse et dans le monde

Астрономические суммы

В списке вредоносного программного обеспечения первое место занимают программы-вымогатели, которые шифруют данные на зараженном устройстве и делают их непригодными для использования до тех пор, пока владелец компьютера не заплатит за код дешифрования. Средняя сумма выкупа сегодня составляет около 230 тыс. долларов, т.е. в четыре раза больше, чем в 2019 году, отметил в интервью телерадиокомпании RTS глава центра информационных технологий компании Kudelski Оливье Шпильман.

Пиратством в виртуальном пространстве занимаются программисты из разных стран мира, в первую очередь – из России, Ирана и Китая, большинство правонарушителей остаются безнаказанными и нечестным путем зарабатывают огромные суммы. По данным Всемирного экономического форума (ВЭФ), в период до 2023 года экономический ущерб от киберпреступлений может составить 5,2 трлн долларов. По оценке исследовательской компании Cybersecurity Ventures, к 2025 году киберпреступность будет «стоять» 10,5 трлн долларов в год.

Жертвы в Конфедерации

Компания Amag, крупнейший швейцарский импортер и продавец автомобилей, чей торговый оборот составил 4 млрд франков в 2020 году, едва не пострадала от виртуальных пиратов. В конце января 2020 года эксперты по ИТ-безопасности Amag зафиксировали попытку кибератаки, после чего все компьютерные сети фирмы были отключены от интернета. Причиной стало зараженное вредоносной программой вложение в электронном письме, которое открыл один из сотрудников, работающих из дома. Это один из любимых способов атаки злоумышленников, тем более что на фоне пандемии резко выросло число людей, работающих дистанционно. Благодаря быстрому реагированию эксперты Amag сумели обезвредить угрозу.

Есть и печальные примеры: в 2019 году компьютеры компании-производителя окон Swisswindows (кантон Тургау), атаковала программа-вымогатель Ryuk, одна из самых распространенных на планете. Все серверы и резервные копии были зашифрованы, сотрудники не могли пользоваться даже электронной почтой. Производитель потерял все контактные данные клиентов и информацию о заказах. К сожалению, резервная копия данных Swisswindows находилась на сервере, который компания использовала ежедневно, к тому же это предприятие не было застраховано от киберрисков.

Руководство Swisswindows отказалось заплатить 800 тыс. франков в биткоинах, полагая, что сможет построить новую ИТ-инфраструктуру. Производство окон было полностью автоматизировано, и в реальности простой затянулся на два месяца. Такого испытания компания не выдержала и обанкротилась, а 170 сотрудникам пришлось искать новую работу.

Свое внимание хакеры обратили даже на производителя часов Swatch Group, из-за чего он столкнулся с серьезными производственными проблемами в сентябре 2020 года. От производителя поездов Stadler Rail преступники потребовали выкуп в размере 6 млн франков, а также украли тысячи внутренних документов. В июле 2019 года пострадала компания-поставщик оборудования для зданий Meier Tobler, в прошлом году хакеры [украли зарплаты](#) преподавателей нескольких вузов Конфедерации.

В мире

В 2020 году в мире утроилось число заражений электронных устройств программами-вымогателями. Во Франции число хакерских атак увеличилось на 543%, в списке жертв – крупные компании, такие как строительный гигант Bouygues (пострадали и его отделения в Швейцарии), а также муниципалитеты и больницы. Производитель GPS-навигационной техники и умных часов Garmin тоже стал целью программы-вымогателя, совсем недавно хакеры атаковали Quanta Computer, одного из основных субподрядчиков компании Apple.

Статистика в Конфедерации

Согласно полицейской статистике, опубликованной в конце марта 2021 года, в Швейцарии в прошлом году было зафиксировано около 24 400 цифровых преступлений. Подавляющее большинство, 16 395 правонарушений, связано с кибермошенничеством.

Что касается частных лиц, то и им достается от злых компьютерных гениев. В Конфедерации находятся доверчивые граждане, которых привлекает реклама в интернете с описанием прибыльных схем инвестирования. Чтобы придать рекламе убедительности, преступники публикуют поддельные интервью со знаменитостями, включая звезду тенниса Роджера Федерера и французского певца Жан-Жака Гольдмана. Кроме того, у швейцарцев выманивают деньги при «доставке» товаров, присваивая их личные данные и т.д. В 2020 году только жители кантона Во потеряли таким образом 15 млн франков, в будущем эта сумма будет расти, поскольку, по словам экспертов, многие не обращаются в полицию, полагая, что она не сможет поймать злоумышленников.

Возвращаясь к обанкротившейся компании Swisswindows, приведем мнение ее бывшего руководителя Неса Мета: предприниматель убежден, что, если не принять меры на политическом уровне, то цифровизация всех сфер нашей жизни будет представлять огромную опасность.

[Швейцария](#) [кибербезопасность](#)

Статьи по теме

[Бум киберпреступности в Швейцарии](#)

[В кантоне Во киберпираты опустошают банковские счета](#)

[В Швейцарии воруют в киберпространстве](#)

[Дистанционная работа и кибербезопасность](#)

[Евгений Касперский: От кибербезопасности к кибериммунитету](#)

[У швейцарских преподавателей украли зарплаты](#)

Source URL:

<https://www.nashagazeta.ch/news/economie/cena-kiberprestupnosti-v-shveyccarii-i-v-mire>