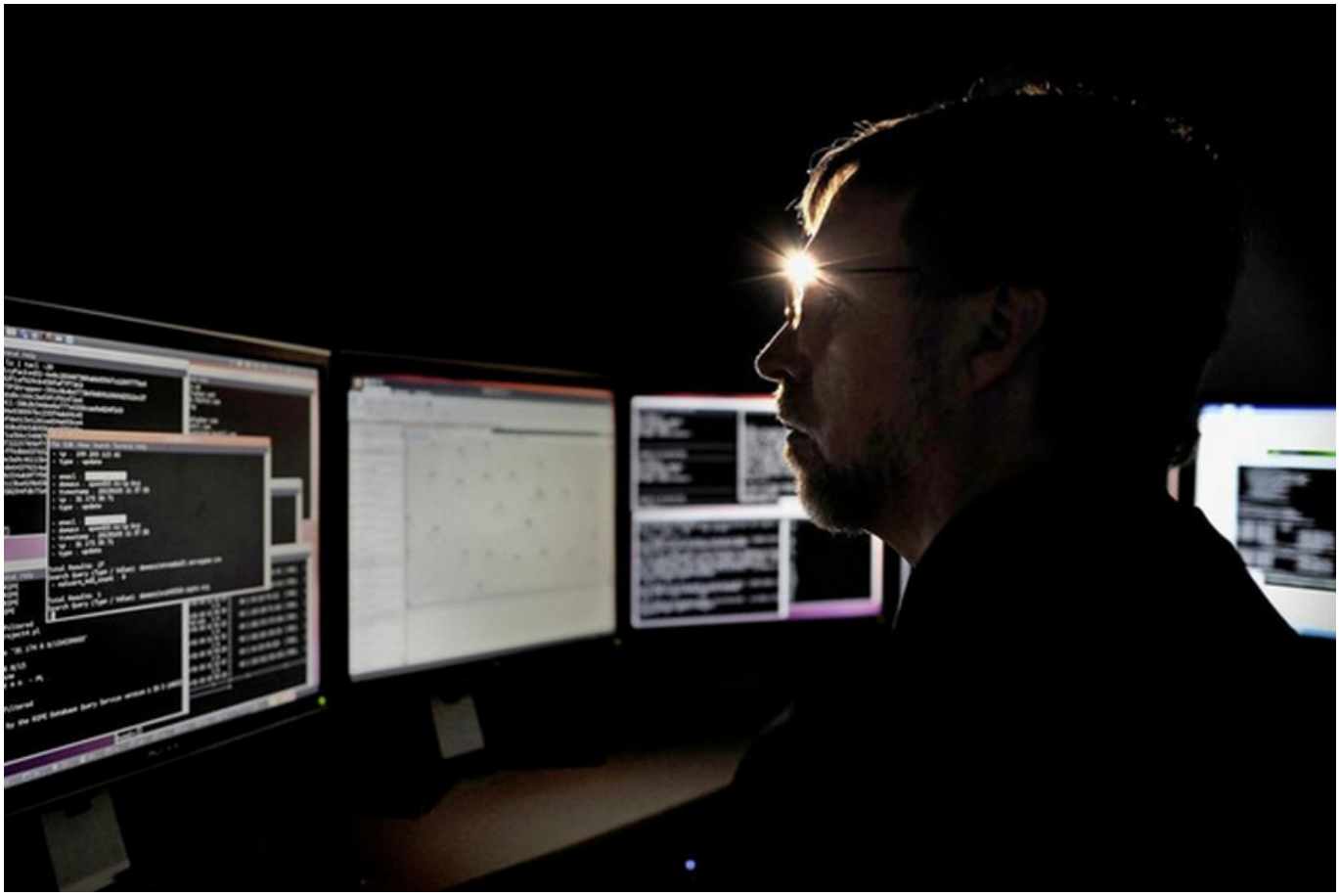
Наша Газета
nashagazeta.ch
Опубликовано на Швейцария: новости на русском языке (https://nashagazeta.ch)

Швейцарские компании почти готовы к отражению кибератак | Les entreprises suisses sont presque prêtes à contrer les cyberattaques

Author: Татьяна Гирко, Базель , 07.02.2017.



(© 24heures.ch)

По данным консалтинговой компании EY, 4 из 10 швейцарских компаний считают себя в состоянии обнаружить, что стали мишенью продвинутой кибератаки.

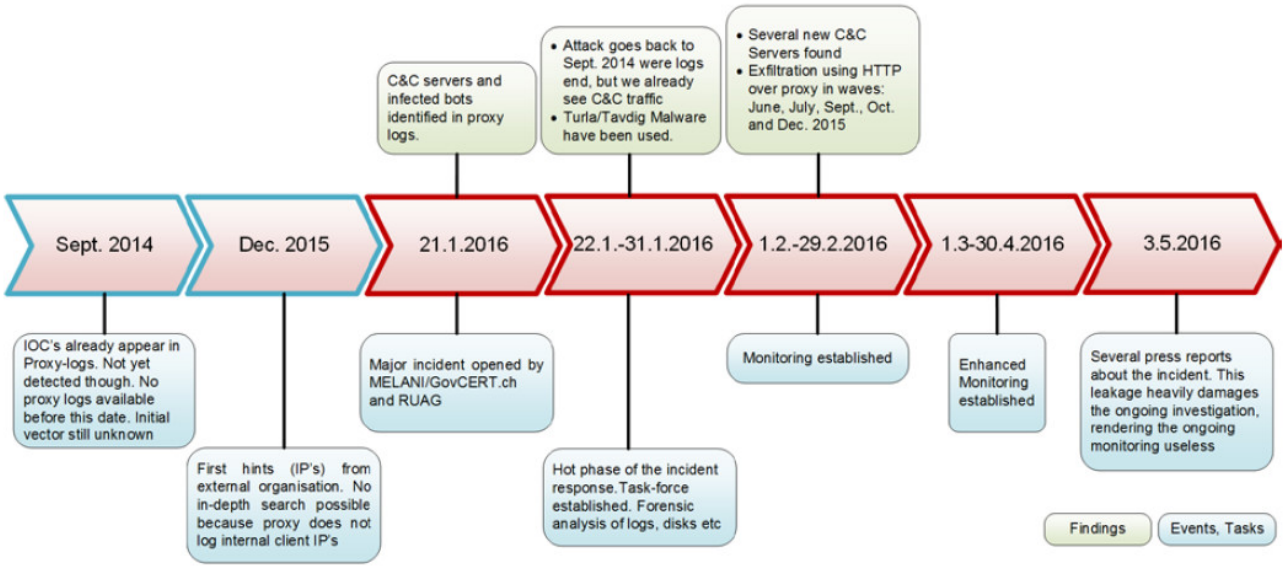
|

Selon EY, 4 sur 10 entreprises suisses considèrent être en mesure de détecter une cyberattaque sophistiquée.

Les entreprises suisses sont presque prêtes à contrer les cyberattaques

Швейцарские компании лучше подготовлены к тому, чтобы предотвращать нападения и противостоять хакерам, но до совершенства в этом вопросе им пока далеко, констатируют авторы 19 по счету Глобального обзора информационной безопасности, публикуемого EY.

Поводом для умеренного оптимизма можно считать тот факт, что, по сравнению с данными предыдущего исследования, сегодня больше швейцарских компаний считают, что ресурсов, которыми они располагают, достаточно для того, чтобы определить, что они стали жертвами продвинутых кибератак. То есть, как минимум, вопросу обеспечения безопасности в этой сфере уделяется должное внимание. Однако о впечатляющих результатах говорить было бы преждевременно: в памяти еще жива масштабная кибератака на компанию оборонного комплекса RUAG, в результате которой в руки хакеров попали более 20 Гб информации. Согласно проведенному по заказу властей Конфедерации расследованию, в этом случае был использован вирус семейства Turla, причем авторы атаки проявили немало терпения, выискивая исключительно интересующие их цели. Объем нанесенного ущерба – во всяком случае пока – оценить не удалось, как и найти авторов и заказчиков этой атаки, при том что речь идет о деле государственной важности. Что же говорить о возможностях обычных компаний?



Как развивалась кибератака на RUAG (скриншот из технического отчета MELANI))

По данным EY, определенное чувство уверенности в готовности отражать атаки киберпреступников руководству швейцарских компаний обеспечивает объем инвестиций, вложенных в программы по изучению киберугроз, позволяющих предотвратить атаки и установить механизмы контроля, центры управления безопасностью и механизмы активной защиты. При этом 84% респондентов считают, что их уровень в этой сфере не полностью соответствует потребностям их компании. Следует отметить, что и киберпираты не стоят на месте, ожидая, пока их приемы будут раскрыты, так что угнаться за развитием этого рынка не так просто.

Авторы исследования, охватывающего 1735 компаний по всему миру (среди которых

49 швейцарских), изучили также основные вызовы, которым вынуждены противостоять участники современной цифровой экосистемы. Несмотря на имеющееся чувство собственной защищенности, компании Конфедерации в прошлом году чаще, чем в 2015-м, сталкивались с теми же основными угрозами. К ним относятся: вредоносные программы/malware, на которые пожаловались 53% респондентов (против 34% годом ранее), фишинг (62% против 41%), отдельной строкой идут кибератаки, направленные на кражу финансовых данных (46% против 22%), обыкновенное мошенничество (47% против 33%) и так называемые уязвимости нулевого дня/zero day, обозначающие новые виды атак, против которых еще не были разработаны защитные механизмы (57% против 45%).

«Компании много предприняли для того, чтобы подготовиться к атакам, но креативность киберпреступников эволюционирует теми же темпами. Поэтому придется удвоить усилия и повысить уровень противодействия. Нужно думать не только о защите и безопасности, но и о «киберсопротивляемости», то есть ответе на уровне системы, позволяющей предотвратить неизбежные случаи и в целом исключить их», – считает Том Шмидт, отвечающий за сферу кибербезопасности в швейцарском подразделении EY.

Кстати, «слабыми звеньями» в обеспечении информационной безопасности респонденты по-прежнему считают небрежность или неосторожность собственных сотрудников (64% против 52% в 2015-м) и уязвимость, связанную с использованием мобильных устройств (41% против 27% в 2015-м). Таким образом, возможно, значение компьютерной грамотности при приеме на работу специалистов любого профиля в ближайшее время возрастет.

Каковы основные препятствия, мешающие швейцарским компаниям в полной мере обезопасить себя от хакеров? На первом месте – бюджетные ограничения (59%). Очевидно, несмотря на тот факт, что киберугроза воспринимается все более серьезно, компании пока не готовы к существенному росту этой статьи расходов: восемь из десяти респондентов не намерены увеличивать финансирование, даже если сами станут мишенью атаки или в подобной ситуации окажутся их конкуренты или поставщики. Вторая проблема заключается в нехватке квалифицированного персонала (53%). Еще один существенный фактор – хотя его роль постепенно снижается – нехватка внимания к проблеме и отсутствие поддержки со стороны руководства (37%).

Обычным пользователям будет интересно узнать, что половина швейцарских компаний в течение недели после атаки, в ходе которой были серьезно скомпрометированы данные, не намерены ставить об этом в известность своих клиентов, а 44% респондентов вообще не имеют коммуникационной стратегии на этот случай. Так что при всей серьезности ситуации, кибератаки пока многих способны застать врасплох.

кибератаки
информационная безопасность
киберпреступность в швейцарии
кибербезопасность
Статьи по теме
Интернет-мошенники действуют под маской швейцарской таможни
Швейцария проявляет интерес к Центру киберзащиты НАТО

Международным компаниям не хватает цифровой безопасности
Джихадизм, Украина и кибербезопасность в центре внимания швейцарских спецслужб
Россияне и марокканцы, обвинявшиеся в фишинге, вышли на свободу

Source URL:
https://nashagazeta.ch/news/economie/shveycarskie-kompanii-pochti-gotovy-k-otrazheniyu-kiberatak