30 000 веб сайтов взламываются ежедневно с целью хищения личных данных или дальнейшего внедрения в корпоративные сети и дата-центры владельцев. Согласно статистике антивирусной компании McAfee и научно-исследовательского центра Center for Strategic and International Studies (CSIS), общий ущерб, нанесённый кибер-преступлениями и интернет-мошенничеством в 2013 году оценивается в 300 миллиардов долларов США. Статистика из Sophos Labs сообщает о 30 000 новых взломах сайтов каждый день, которые распространяют злонамеренный контент и вирусы с целью инфицирования своих посетителей. Многие ИТ-интеграторы поставляют в компании заведомо неэффективные решения по обеспечению ИТ-безопасности, которые приносят им существенный доход, а учитывая немалую загрузку ежедневной работой ИТ отделы зачастую берут тот продукт, который нахваливает интегратор. Немалую роль сыграл и экономический кризис, от которого многие компании еще до сих пор полностью не оправились и продолжают экономить на ИТ, урезая в первую очередь расходы на безопасность. Ситуация усугубляется плохим взаимодействием руководства компаний и ИТ-отделов, которые зачастую «говорят на разных языках» и преследуют разные цели. В итоге, руководство попросту не может достоверно проверить, насколько эффективно защищен их бизнес в Сети.

В последнее время особенно участились атаки на веб-сайты и веб-приложения, которые все чаще становятся «открытой дверью» в корпоративную сеть. Новые технологии все больше используют простые, удобные и понятные веб интерфейсы, защите которых не уделяется должного внимания, что приводит к их взлому и последующей компрометации стоящих за ними баз данных. Очень часто взламываются веб-сайты даже тех компаний, у которых на сайте вообще нет никакой ценной информации и которые полностью изолированы от внутренних корпоративных сетей, в следствии чего безопасности таких сайтов уделяется категорически мало времени. Этим успешно пользуются хакеры, размещая на сайте вредоносный код и отправляя ссылки на инфицированный корпоративный сайт сотрудникам компании, которые с очень большой вероятностью последуют ссылке, ведущей на их сайт. В результате это позволит злоумышленникам проникнуть в их компьютер и «пойти» дальше по корпоративной сети.

Инновационное решение проблемы безопасности веб сайтов анонсировала Швейцарская компания High-Tech Bridge, которая довольно часто мелькала на первых полосах международных СМИ в последнее время. В сентябре 2013 сотрудники компания вынудили американского гиганта Yahoo кардинально пересмотреть программу вознаграждения за найденные уязвимости, когда сообщив Yahoo о 4 уязвимостях позволяющих украсть любой почтовый адрес на Yahoo, они получили взамен 12 долларов и 50 центов. В самом начале 2014 года, имя компании не сходило со страниц журналистов, после того как в США подали многомиллиардный коллективный иск против социальной сети Facebook, которая, как это ранее смогли доказать исследователи High-Tech Bridge, перехватывает личные сообщения пользователей социальной сети. Недавно, очередное исследование компании встряхнуло Всемирный Экономический Форум (World Economic Forum), организаторы которого получили уведомление от High-Tech Bridge об опасной бреши на своем веб-сайте, раскрывающей десятки тысяч частных email-адресов всех VIP участников форума, и даже не удосужились закрыть уязвимость или ответить на оповещение.