**Защищаться намного сложнее, чем атаковать?**

Однажды я писал, что получить популярность взломом намного проще, чем защитой. Хакеры, взломавшие сервера, быстрее становятся знаменитыми и на это есть множество причин. Сегодня я решил снова затронуть эту тему немного с другой стороны.

Первая, и самая глупая причина – пипл хавает все плохое. Тут имеется ввиду не только то, что хакеры больше любят взламывать, но и то, что массы любят слышать плохие новости, криминал и что-то неординарное. Поэтому и журналисты средств массовой информации с удовольствием раздувают скандалы в прессе, если какой-то пионер взломает сервер или сделает еще что-то плохое.

Если же какой-то хакер или администратор смог отразить целый миллион атак за час, никто об этом не узнает. Такая новость не будет интересовать пипл, а значит, ни один журналист не нажмет ни одной клавиши в текстовом редакторе ради такой новости. И что неординарного в том, что кто-то хорошо выполняет свою работу? Ничего. Администраторы должны защищать сервера и это их обязанность, а то, что кто-то делает это хорошо, не стоит публикаций в прессе. Никто не будет писать статью или делать целую передачу на телевидении ради какой-то доярки, которая каждый день доит корову и ничего неординарного не происходит. А жаль. Жаль, что когда человек выполняет свою работу добросовестно, никто этого не замечает.

Вторая причина, по которой взламывать намного проще – администратору достаточно совершить только одну ошибку и если взломщик найдет ее, то администратор становиться в неловкое положение. Администратор – он же как сапер, только многоразовый ☺. Если произошел взрыв, то у сапера шансов выжить не так много. Администратор после взлома тоже получает своеобразный взрыв, особенно, если данные уничтожаются. Этот взрыв может даже лишить человека работы. И все же он остается жив и может закрыть уязвимость или даже найти новую работу и продолжать войну против взломщиков до следующего взрыва.

Администратор должен защищать систему в целом, он должен следить за каждой дверью и окном. Но если он упустит хотя бы одну щелку, взломщик сможет проникнуть в систему. Взломщику не нужно знать систему целиком и полностью, он не обязан быть гением и знать все уязвимости. Достаточно знать только одну уязвимость, и если администратор не знает этого или просто повезло, взлом произойдет.

Отсюда можно выделить еще одну причину, – по которой администраторы находятся в более сложном положении. Они должны следить за системой постоянно и 24 часа в сутки. Если на рынке появляется новая уязвимость, то администратор должен среагировать моментально и закрыть все потенциальные входы. Тут можно прозевать и этот зевок может дорогого стоить. Взломщиков в сети миллионы и при появлении вкусной дырки, все они бросаются на сервера с целью проникновения внутрь.

Хакеры постоянно находят новые уязвимости и самое страшное, что первое время уязвимость доступна только хакерам и они могут ее использовать, пока производитель дырявого софта не выпустит обновление с исправлением. В зависимости от производителя и суровости ошибки, время от публикации уязвимости до появления исправления может быть очень большим.