Жизнь после "Пети" — как вирус повлиял на безопасность ОТП Банка
Delo.ua, 14.02.2018
https://delo.ua/special/zhizn-posle-peti-kak-virus-povlijal-na-bezopasnost-otp-banka-339097/

Дмитрий Янишевский
начальник управления информационной безопасности, ОТП Банк

Жизнь после "Пети" — как вирус повлиял на безопасность ОТП Банка

Начальник управления информационной безопасности ОТП Банка — о победе над самым нашумевшим вирусом в Украине

27 июня сотни украинских компаний подверглись масштабной кибератаке посредством вируса, который в Украине получил название Petya.A или "Петя". Пострадали очень многие: от "Новой Почты" до аэропорта "Борисполь", крупные и мелкие компании, большинство банков. Среди них оказался и ОТП Банк.

Мы, как и многие в тот день, "упали", но, в отличие от других компаний, быстро "поднялись". Факт атаки был выявлен практически мгновенно системами мониторинга, что позволило нам очень быстро отреагировать. Благодаря быстрой реакции основные банковские операционные системы не пострадали. Основная проблема была в том, что пострадали рабочие станции, через которые люди подключаются к банковским системам. Все сотрудники мгновенно включились в работу. Основные инфраструктурные элементы не пострадали во время атаки, все остальное было восстановлено из резервных копий. Даже при наличии определенных слабых мест в защите, все системы и сотрудники сработали так, что банк практически не понес прямых убытков. В определенном смысле нам очень повезло.

Уже на следующий рабочий день банк полностью смог восстановить работоспособность всех систем и продолжить операционную деятельность. Не побоюсь преувеличения — это очень высокий показатель при такого рода атаке.

Тем не менее вирус Petya был далеко не первой кибератакой на банковскую систему. Все предыдущие, последняя из которых была в мае, мы успешно отражали. Особенность "Пети" состояла в том, что он использовал для поражения один из немногих доверенных, монопольных сервисов, предназначенных для отправки отчетности в государственные органы, от которых мы и сегодня не можем отказаться.

Но, несмотря на ущерб, атака выявила слабые и сильные стороны нашей системы защиты. В итоге — слабые места закрыты, проводятся мероприятия по усилению действующих механизмов защиты, внедрению дополнительных. Проведено определенное организационное усиление системы управления информационной безопасностью.

Фактически во время атаки "Пети" мы протестировали наш business continuity план в действии — то есть мероприятия по обеспечению непрерывности бизнес-деятельности, в том числе по оперативному восстановлению работоспособности ИТ-систем. Лучше сценария, наверное, не придумаешь.

В будущем уровень киберугроз и их частота с большой вероятностью будут только возрастать. Поэтому даже после того как мы справились с такой сложной атакой, останавливаться нельзя. Мы постоянно анализируем информацию об угрозах, поступающую к нам из разных источников как бесплатных, так и коммерческих (threat intelligence activity). А так как стопроцентно спрогнозировать будущие атаки невозможно, наша основная задача — обеспечить живучесть корпоративной сети банка в условиях неопределенности вектора атаки.

Банк уже показал, что может эффективно и быстро восстанавливать работоспособность своих систем. Кроме того, разработаны и протестированы дополнительные протоколы реагирования, задачей которых является обеспечение максимально быстрой реакции на угрозу кибератаки, изоляция сегментов сети, находящихся в зоне высокого риска.

Жизнь после "Пети" — как вирус повлиял на безопасность ОТП Банка
Delo.ua, 14.02.2018
https://delo.ua/special/zhizn-posle-peti-kak-virus-povlijal-na-bezopasnost-otp-banka-339097/

Мы постоянно обмениваемся информацией и опытом с другими банками и НБУ. Для этого существует ряд площадок, форумов, в НБУ регулярно проводятся обучающие мероприятия. Существует утвержденная стратегия информационной безопасности Украины, в рамках которой все банки участвуют под эгидой НБУ в киберзащите критической инфраструктуры в банковской сфере.

Кибератаки — это неизбежность для публичных компаний, атака, подобная "Пете", не первая и не последняя. Стопроцентной защиты не существует, кто-бы ни пытался утверждать обратное. Основное внимание в данном контексте следует уделять повышению живучести и отказоустойчивости критических элементов информационной инфраструктуры и средствам раннего обнаружения атак.