**Цифровизация компаний как катализатор киберпреступности**

Степень цифровизации бизнесов с каждым годом растёт. Это влечёт за собой большое число преимуществ, но есть и обратная сторона этого процесса – хакерские атаки. И зачастую они приводят к репутационным и финансовым потерям. Причина – пренебрежение правилами кибергигиены.

Главные проблемы, которые наиболее часто выявляются в результате аудитов безопасности IT-инфраструктуры, таковы: необновлённый софт, отсутствует культура патч-менеджмента, дырявый периметр. Результат – увеличение числа кибератак. По данным компании Positive Technologies, в течение 2019 года количество хакерских атак повышалось из квартала в квартал.

**Теперь об APT-атаках знают все**

APT-атака (от advanced persistent threat) – профессионально подготовленное и грамотно спланированное целенаправленное кибернападение на IT-инфраструктуру фирмы или даже отрасли промышленности. Зачастую их осуществляют ОПГ, в арсенале которых имеются серьёзные финансовые ресурсы и технические средства. Кибератаки очень опасны для коммерческих структур, поскольку многие из них просто не могут им противодействовать.

В 2019 году количество АРТ-атак было значительно выше по сравнению с числом массовых атак. Их доля составила 59,5 процента. Многие руководители бизнесов осознают опасность, связанную с кибератаками, и сегодня всё чаще для решения вопросов обеспечения информационной безопасности привлекается топ-менеджеры. Они понимают, что невозможно создать непробиваемую броню против хакерских атак. Здесь существуют всего два варианта: большую часть систем безопасности или уже взломали, или взломают в будущем. Из этого вытекают главные задачи эффективной системы безопасности: быстрое обнаружение кибератаки и минимизация ущерба.

Для специалистов не является секретом, что уже длительное время киберпреступникам удается контролировать много компаний, которые даже не догадываются об этом. В качестве примера можно привести случай, когда кибергруппировка TaskMasters, обнаруженная в 2019 году, контролировала корпоративную IT-инфраструктуру в течение восьми лет.

Следует констатировать, что наметился положительный тренд: многие фирмы стали интересоваться вопросами, связанными с обеспечением информационной безопасности, обнаруживать киберинциденты в своей IT-инфраструктуре, анализировать хакерские атаки.

Однако есть и негативный тренд: хакеры с каждым годом всё увереннее себя чувствуют в информационном пространстве, а из-за наличия в широком доступе большого количества обучающих материалов по взлому информационных систем порог входа в киберпреступность очень низкий.

К сожалению, госпрограммы по повышению осведомленности населения в вопросах информационной безопасности не существует. Из-за этого хакерам удаётся обманывать доверчивых людей. До тех пор, пока не найдётся эффективного решения этой проблемы, организаторы кибератак и дальше будут зарабатывать деньги и планировать новые преступления.

**Чего хотят киберпреступники?**

В подавляющем большинстве случаев злоумышленники хотят украсть ценную информацию (доля подобных преступлений по итогам четвёртого квартала прошлого года составляет 69 процентов). Также они стремятся получить финансовую выгоду. На третьем месте в этом списке – хактивизм (проникновение в компьютерные сети для распространения различных идей). Последнее место занимает кибервойна.

В основном мошенники стремятся заполучить данные платёжных карт и персональную информацию. Главные цели APT-группировок – фирмы, которые владеют ценными сведениями и денежными средствами. Следует отметить, что жертвами кибернападений могут быть не только представители крупного бизнеса, но и малые и средние предприятия Последних используют в качестве плацдарма для атак на крупный бизнес и для маскировки киберпреступлений. Под пристальным вниманием преступников находятся и вендинговые компании, и провайдеры услуг связи, и иные поставщики услуг. Организация даже может не подозревать о том, что от её данных исходит угроза.

В качестве примера можно привести случай из практики фирмы Positive Technologies: крупная организация была атакована через вендинговый автомат. Поставщик торговых автоматов попросил предоставить удалённый доступ к автомату. Оборудование подключили к корпоративной сети, посредством которой обеспечивался доступ к интернету для функционирования вендингового аппарата и связь с серверами управляющей организации. Результат: через этот канал связи была совершена кибератака.

Компрометация фирмы может быть одним из этапов в преступной хакерской схеме, когда главной целью киберпреступников является получение доступа к почтовому домену (это позволит осуществлять рассылку писем от лица организации), кодам ПО (для внедрения вредоносного скрипта) и инфраструктуре клиентов или контрагентов.

Зачастую злоумышленники производят кибератаки посредством использования доверенных источников (поставщики оборудования, имеющие менее защищённую IT-инфраструктуру, клиенты и т.д.). Это значительно снижает киберзащищённость организаций. Фишинг такого вида использовали такие известные хакерские группировки, как TaskMasters, Cobalt, RTM. Они весьма коварны: атакуют быстро и дерзко, часто производят смену инструментария и тактики, чтобы закрепиться в IT-инфраструктуре и предотвратить обнаружение.

**Контрагент не так защищён, как хотелось бы**

Лёгкая добыча для киберпреступности – небольшие и средние фирмы, которые не готовы в необходимом размере вкладывать денежные средства в свою информационную безопасность. По мере совершенствования систем защиты крупного бизнеса от хакерских нападений хакеры всё чаще будут применять наиболее коварный фишинг, создавать более продвинутые версии вредоносного ПО и взламывать фирмы со слабой защитой, делая из них удобные плацдармы для нападения на крупные бизнес-структуры.

Специалисты прогнозируют увеличение популярности продаж доступов к взломанным сетям. Хакеры всё чаще, взломав корпоративную сеть, будут продавать или сдавать в аренду доступ к ней третьим лицам. Стоимость доступа к сотням узлам в сети может составлять три-пять тысяч долларов, а стоимость абсолютного контроля над сетью – двадцать тысяч долларов и выше.

**Как защититься от киберугроз?**

Российские фирмы повсеместно используют стандартные решения для защиты от угроз, однако с применением специальных защитных средств от хорошо спланированных и многоэтапных кибератак дела обстоят гораздо хуже.

*Методы противодействия:*

**1.** Необходимо регулярно проводить ретроспективный анализ и перепроверять почтовые вложения и иные файлы с применением вновь выявленных индикаторов компрометации. Это позволит своевременно находить артефакты, которые будут указывать на злоумышленников.

**2.** Нужны высококлассные специалисты, которые будут:

* Настраивать и контролировать работу технических средств защиты.
* Собирать и обрабатывать данные о событиях безопасности.
* Анализировать трафик и искать необычную активность в инфраструктуре.
* Своевременно реагировать на киберинциденты и быстро восстанавливать информационные системы.

**3.** Нужно повышать знания персонала в сфере информационной безопасности.