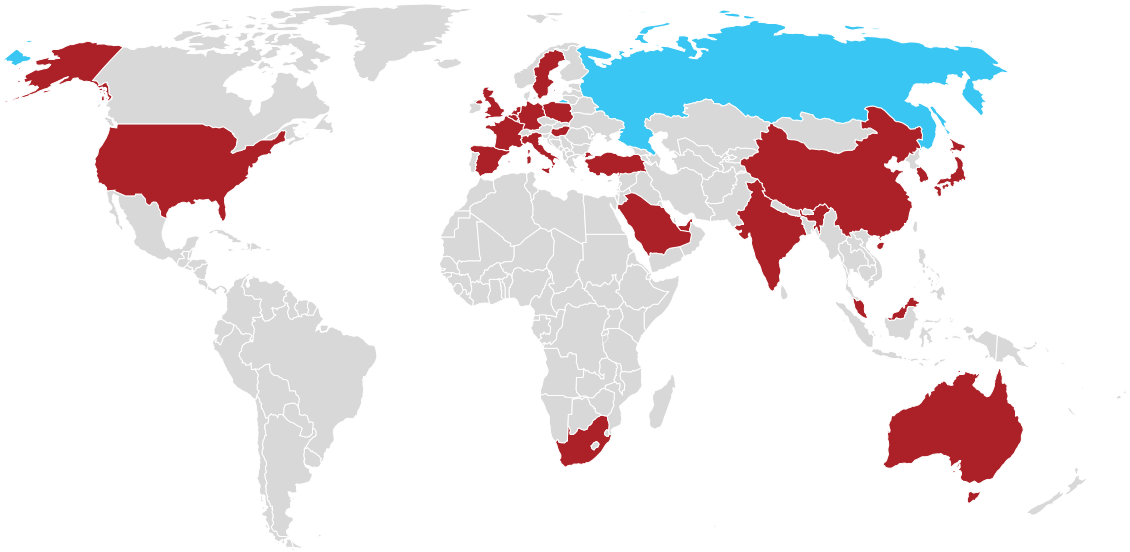
Устойчивость компаний к киберугрозам и зловредному ПО.

Содержание

Цифровая трансформация, и особенно внедрение облачных технологий, ускорились из-за глобальной пандемии. В связи с необходимостью поддержки удаленной работы предприятия столкнулись с необходимостью переноса своих приложений из собственных центров обработки данных в облако. Новый глобальный опрос почти 2700 ИТ-руководителей и специалистов в 21 стране, проведенный Wakefield Research по заказу Veritas Technologies, показал, что по мере ускорения этого перехода уменьшается устойчивость к атакам вирусов-вымогателей, зловредному ПО и другим киберугрозам. На то есть множество причин, но главная состоит в том, что предприятия расширяя использование облаков, которые являются простой в использовании платформой для запуска приложений и хранения информации, недостаточно принимают мер по организации отказоустойчивости при данном подходе. Компаниям необходимо обратить пристальное внимание на этот пробел, позаботившись об организации отказоустойчивости облачных платформ и сохраности данных, чтобы идти в ногу с растущей сложностью современных ИТ.



VERITAS

Данные по России

Многие предприятия в России становятся уязвимы к киберугрозам, в результате чего критически важные для бизнеса данные становятся доступны программам-вымогателям. Поскольку организации внедряют все больше облачных платформ, повышая сложность ИТ, системы безопасности перестают соответствовать уровню сложности информационных сред. В России примерно четыре респондента из десяти заявляют, что их компания подверглась атаке программ-вымогателей. В итоге, многие из них сталкиваются с перспективой длительных перебоев в работе или потери данных в случае атаки программы-вымогателя.

Сложность ИТ

- 35 % предприятий используют равное сочетание общедоступного и частного облака, а еще 25 % используют в основном внешнее облако, но по-прежнему сохраняют часть своих данных и приложений локально. На глобальном уровне это соотношение составляет 36 % и 25 % соответственно.
- Российские компании в среднем используют около 11 облачных сервисов (IaaS, PaaS и SaaS), что аналогично количеству в регионе EMEA, причем 54 % используют более 5.

Где ваша организация хранит большую часть своих данных и приложений?

- Такое использование облака усложняет ИТ. 62 % российских респондентов заявили, что меры безопасности их предприятий не соответствуют сложности их ИТ-инфраструктуры.

- Главные опасения российских ИТ-руководителей по поводу чрезмерной сложности ИТ аналогичны таковым в регионе EMEA, хотя российские предприятия больше своих коллег из региона EMEA обеспокоены тем, что сотрудники имеют доступ к файлам, к которым не должны иметь доступа, или не имеют доступа к нужным файлам.

Главные опасения российских ИТ-руководителей по поводу чрезмерной сложности ИТ:

42% Наличие у сотрудников доступа к файлам, которые им не нужны, или отсутствие доступа к нужным файлам

38% Повышенный риск внешних атак, таких как утечка данных и программы-вымогатели

36% Возможность потери данных

Главные опасения ИТ-руководителей в регионе EMEA по поводу чрезмерной сложности ИТ:

37% Повышенный риск внешних атак, таких как утечка данных и программы-вымогатели

36% Повышенный риск внутренних атак (утечки, ошибки сотрудников, должностное злоупотребление и т. д.)

35% Возможность потери данных

- Предприятиям в России приходится делать больше при меньших ресурсах, чтобы восполнить пробелы в отказоустойчивости, и только 36 % респондентов заявили, что их компания увеличила свой бюджет на ИТ-безопасность с начала пандемии COVID-19.

Воздействие программ-вымогателей

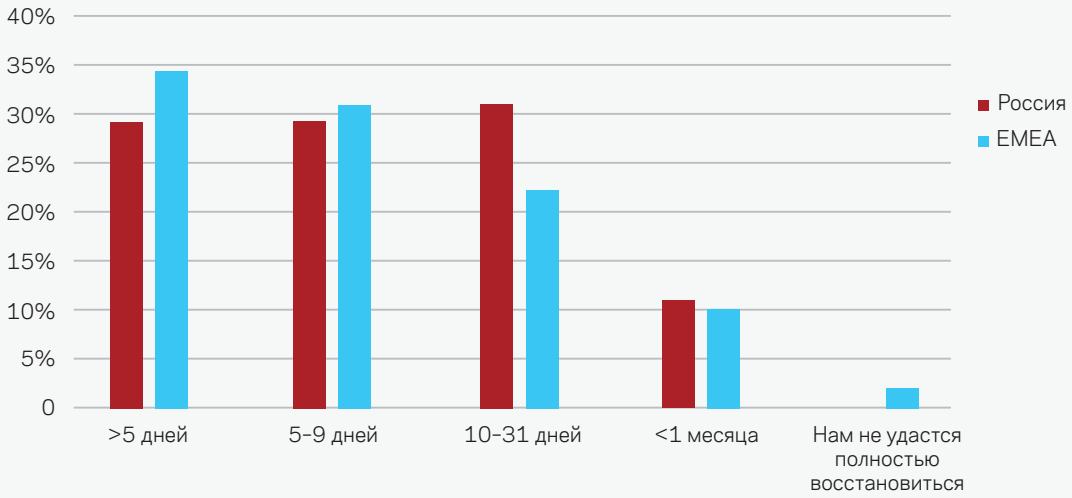
- Программы-вымогатели представляют собой растущую угрозу. 43 % российских респондентов заявили, что сталкивались с атаками программ-вымогателей, при этом среднее количество атак было равно 5; глобальный показатель составляет 42 % и 4,5 атаки.
- Довольно много предприятий в России расплачиваются за недостаточную отказоустойчивость. Так как их системы резервного копирования и восстановления недостаточно надежны, при атаке программ-вымогателей у российских компаний часто нет другого выбора, кроме как заплатить выкуп. Среди тех, кто столкнулся с атакой программ-вымогателей, 35 % российских респондентов заявили, что их компания заплатила выкуп полностью или частично; этот показатель составил 54 % в регионе EMEA и 60 % респондентов во всем мире.

VERITAS

Пробел в устойчивости к киберугрозам

- Российские предприятия так же испытывают недостаток устойчивости, как и их коллеги во всем мире. 71 % российских респондентов (65 % во всем мире) считает, что для полного восстановления после атаки программы-вымогателя потребуется 5 дней или больше.

Сколько времени потребуется для восстановления после атаки программы-вымогателя (если вы не заплатили выкуп)?



- Только 15 % российских респондентов заявили, что их компания следует рекомендуемой передовой практике: иметь три копии своих данных, при этом одну из них — вне офиса без доступа в Интернет. Еще 22 % российских респондентов заявили, что у их компании есть три или более копий их данных на месте, но это означает, что почти две трети опрошенных предприятий не имеют передовой стратегии для резервного копирования своих данных.
- Российские организации недостаточно тестируют свой план аварийного восстановления: только 34 % тестировали его за последние два месяца по сравнению с 43 % во всем мире.

Рекомендация для России: Усилить меры по организации отказоустойчивости ИТ инфраструктуры и сохранности данных. Почти две трети организаций заявляют, что их меры безопасности не соответствуют усложняющейся ИТ-инфраструктуре, только 37 % имеют три копии своих данных, и всего 13 % тестировали свои системы аварийного восстановления за последние 30 дней по сравнению с 15 % во всем мире. Тот факт, что российские компании, подвергшиеся атакам программ-вымогателей, столкнулись в среднем с 5 атаками, указывает на то, что этим компаниям необходимо сосредоточиться на планировании отказоустойчивости или же вовсе пересмотреть подход к сохранности данных. Компаниям в России необходимо как можно скорее восполнить пробелы в устойчивости к киберугрозам, чтобы получить возможность восстановить свои данные, не платя выкуп. Организациям в России следует рассмотреть использование более надежных методов защиты от атак программ-вымогателей. К ним относятся:

- **Комплексный обзор стратегии:** предприятиям в России следует пересмотреть свою стратегию отказоустойчивости с точки зрения обеспечения наглядности, мониторинга и автоматизации восстановления в реальном времени.
- **Более надежное резервное копирование:** компании должны следовать подходу к резервному копированию «3-2-1»: как минимум три копии данных в двух разных местах, с по крайней мере одной за пределами офиса.
- **Более частое тестирование аварийного восстановления:** в идеале предприятиям следует тестировать свой план аварийного восстановления один раз в месяц. Картина их данных и приложений меняется так быстро, что менее частые тестирования могут привести к сбою сайта аварийного восстановления в случае необходимости.
- **Регулярное обновление систем безопасности:** ИТ-команды должны быть в курсе обновлений и дополнений к приложениям, касающихся ИТ безопасности.
- **Шифрование данных:** предприятиям следует внедрить шифрование данных для их защиты при передаче по любой сети.
- **Неизменяемое хранилище:** ИТ-специалисты должны использовать технологию неизменяемого и нестираемого хранилища, чтобы предотвратить шифрование или удаление резервных копий программами-вымогателями.
- **Управление доступом**: внедрение контроля доступа на основе ролей и ограничение доступа только необходимыми функциями для отдельных пользователей.

VERITAS