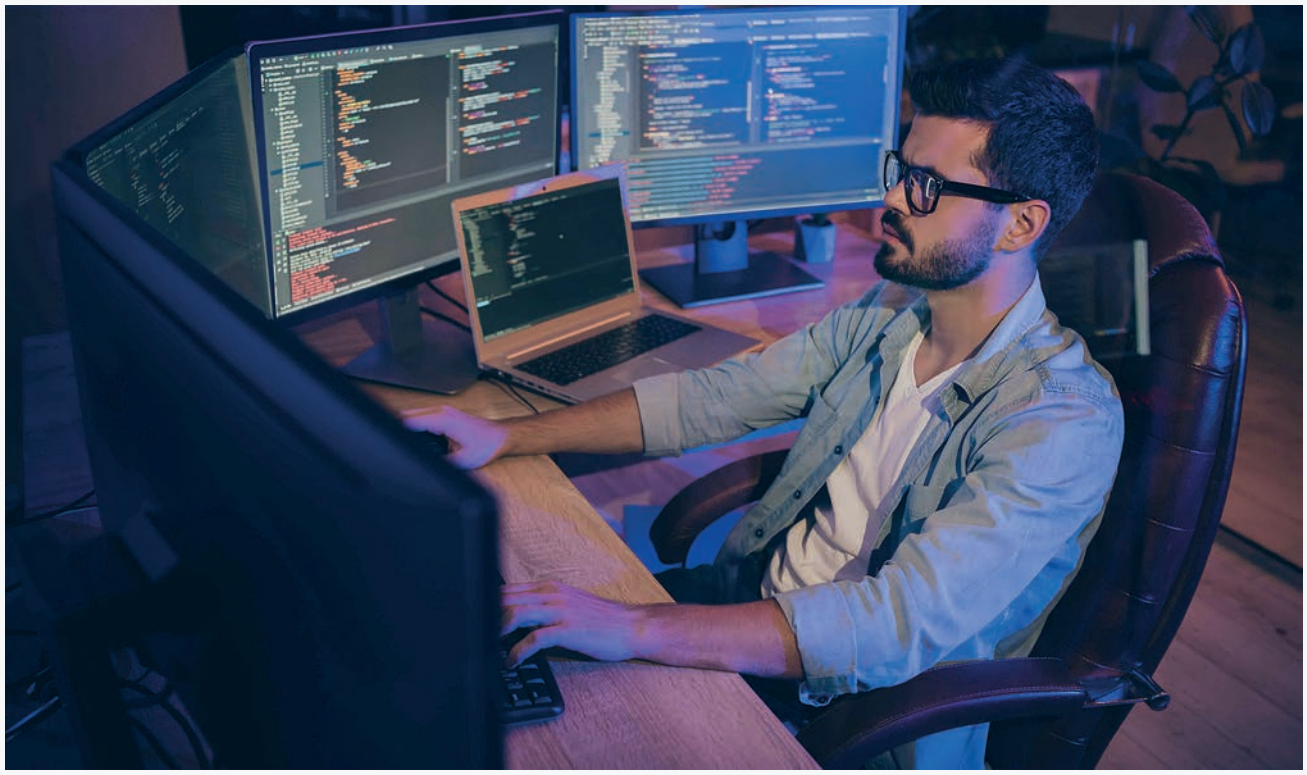
Сервисный ответ киберугрозам

«Ростелеком-Солар» представил в Краснодаре сервисы информационной безопасности для бизнеса и государственных структур

Дочерняя компания ПАО «Ростелеком» организовала для сотрудников IT-сферы и руководителей крупных компаний роуд-шоу «КиберДрайв», на котором эксперты рассказали об обеспечении безопасности в условиях растущих киберугроз. По данным «Ростелеком-Солар», в прошлом году в Южном федеральном округе было выявлено 61 тыс. киберпреступлений.



Злоумышленники адаптировались к пандемии

«2020 год был удивительным с точки зрения безопасности. Основным катализатором изменений на рынке стал переход компаний на удаленный режим работы. Это очень сильно сказалось на количестве инцидентов в киберпространстве, которые мы фиксируем. В целом по России этот показатель составил 1,9 млн, рост по сравнению с 2019 годом феноменальный — 73%. Также выросла доля критичных инцидентов (+20%)»,— сообщил пресейл-консультант продуктов и сервисов Solar JSOC ПАО «Ростелеком» Алексей Касьянов.

Согласно собранной «Ростелеком-Солар» статистике, около 35% всех кибератак приходится на внедрение вредоносного программного обеспечения. Внутри этого сегмента наибольший прирост показывает применение так называемых шифровальщиков. Второе место за атаками на web-ресурсы — 34%. «На момент первой волны коронавируса в 2020 году мы фиксировали двукратный рост таких атак. Это говорит о том, что злоумышленники адаптируются под изменяющуюся среду»,— рассказал Алексей Касьянов.

На долю brute force-компрометации (метод угадывания, предполагающий систематический перебор всех возможных комбинаций символов до тех пор, пока не будет найдена правильная комбинация) пришлось 14% попыток взлома.

При переходе компаний на удаленный режим работы их информационный периметр неизбежно расширяется, это становится серьезным вызовом в сфере информационной безопасности для бизнеса. Злоумышленники ломают домашние маршрутизаторы сотрудников, а также общедоступные Wi-Fi-сети, после чего попадают внутрь периметра компаний. На безопасности также сказывается такой фактор, как низкая защищенность домашних ПК, ведь далеко не каждая организация во время пандемии предоставила сотрудникам корпоративные ноутбуки. Очень популярны в 2020 году были атаки с использованием RDP (протокол удаленного рабочего стола). Чтобы обеспечить удаленную работу, компании делали порты общедоступными, злоумышленники пользовались этим, применяя для взлома автоматизированные боты.

Сегодня 75% атак киберперступников начинается с фишинга. Это основной способ доставки вредоносного ПО в корпоративные сети. Человеческий фактор имеет здесь первостепенное значение. «2020 год был благосклонен к этому виду атак из-за удаленки. Более того, тема COVID-19 стала самой популярной темой фишинга»,— отметил Алексей Касьянов.

В 2020 году был зафиксирован рекордный прирост атак через подрядные организации. Злоумышленники ведут атаки либо через компании, которые оказывают бизнесу услуги на аутсорсинге, или же через организации, реализующие собственные программные решения.

Уязвимости — это отдельная большая глава в российской информационной безопасности. Практически ни одну сложную атаку сегодня невозможно представить без их использования. Самой популярной уязвимостью в 2020 году стала Zelogon CVE-2020-1472 (этот баг позволяет захватывать Windows-серверы, работающие в качестве контроллеров домена в корпоративных сетях). Новая популярная уязвимость уже 2021 года — Exchang CVE-2021-26855 (позволяет внешнему атакующему обойти механизм аутентификации в MS Exchange и выдать себя за любого пользователя).

«От нее уже пострадало большое количество компаний, в том числе и в России. К сожалению, уязвимости в корпоративном сегменте закрываются очень долго. Даже у организаций, где работают опытные специалисты, на их ликвидацию уходит от 3-4 недель, что уж говорить об обычных компаниях, где порой уязвимости не закрываются вообще»,— рассказал Алексей Касьянов.

Подводя итог своему выступлению, эксперт отметил, что сегодня количество киберугроз значительно выросло, злоумышленники стали точнее, а вредоносное ПО, которые они используют,— эффективнее. При этом менее 30% компаний сегодня могут эффективно сопротивляться современным вызовам.

В 2020 году был зафиксирован рекордный прирост атак через подрядные организации. Злоумышленники ведут атаки либо через компании, которые оказывают бизнесу услуги на аутсорсинге, или же через организации, реализующие собственные программные решения

Экосреда для безопасности

В борьбе с киберугрзами «Ростелеком-Солар» предлагает сервисную модель решения проблемы. Предложение компании представлено направлениями Solar MSS и Solar JSOC.

По словам директора по развитию бизнеса по информационной безопасности «Ростелекома» на Юге Павла Переверзева, именно сервисная модель является наиболее оптимальной для бизнеса, поскольку снижает финансовую нагрузку при гарантированном результате. «Применение собственных решений в сфере информационной безопасности накладывает на заказчика, помимо основных затрат на их приобретение и внедрение, ряд скрытых затрат, которые влияют на экономику организации, но при этом незаметны в долгосрочной перспективе. В будущем потребуется обновление ПО, продление лицензии, дополнительная техническая поддержка, ремонт оборудования. Сервисная модель предполагает, что большая часть работ, связанная с обслуживанием и реализацией функционала сервисов, осуществляется нашими специалистами, освобождая сотрудников заказчика от рутинной работы»,— рассказал Павел Переверзев.

По его словам, «Ростелеком» присутствует во всех регионах России, что обеспечивает компании живой контакт с заказчиками. Представителям бизнеса нет необходимости обращаться к подрядчикам, находящимся в других регионах. В пяти субъектах страны у компании есть собственные центры мониторинга, которые реагируют на инциденты информационной безопасности. Они работают в формате 24/7 круглый год и присутствуют практически во всех часовых поясах.

«Одно из наших преимуществ — доступность. Сервис можно подключить довольно быстро, а при необходимости также быстро его масштабировать. Срок развертывания составляет до двух дней»,— отметил Павел Переверзев.

Сервис Solar MSS представляет большое количество решений в сфере кибербезопасности — защита от сетевых угроз (защита цифрового периметра организации), защита веб-приложений от высокоуровневых атак, защита электронной почты от вредоносных вложений, а также от фишинговой активности, контентная фильтрация. Также в Solar MSS присутствует сервис защищенной удаленной работы и защита от DDoS-атак — это классическое решение, которое может обеспечить стабильность доступа пользователей к электронным площадкам, через которые осуществляется работа бизнеса. Сервис шифрования каналов связи работает на базе ГОСТ VPN, он интересен тем, что реализуется на оборудовании ведущих отечественных производителей и обеспечивает соответствие действующим требованиям законодательства в сфере информационной безопасности. Также Solar MSS предлагает своим клиентам такую услугу, как управление навыками информационной безопасности. Она дает возможность обеспечить базовый уровень безопасности через обучение сотрудников компаний, которое проходит в несколько этапов и завершается контрольными тестами.

Осуществляет Solar MSS и контроль уязвимостей, этот сервис позволяет провести оценку безопасности электронных площадок, приложений, информационного контура с последующим выявлением уязвимостей и предоставлением развернутого отчета.

Управление сервисом Solar MSS осуществляется через личный кабинет, который позволяет контактировать с сотрудниками техподдержки, подключать новые сервисы, гибко настраивать их производительность.

Еще одно сервисное направление «Ростелекома» — Solar JSOC, которое реализуется на базе центров мониторинга. Это высокоуровневые сервисы, которые позволяют в полном объеме закрыть потребности компаний, начиная от мониторинга реагирования на события и инциденты информационной безопасности, заканчивая построением собственных SOC-центров и осуществлением взаимодействия с ГосСОПКА (государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации).

Преимущество сервиса заключается в том, что он реализуется собственными сотрудниками компании, которые имеют подтвержденные сертификаты по различным направлениям информационной безопасности.

Как рассказал представитель ООО «РТК-сервис» Сергей Очаковский, компания сейчас рассматривает внедрение именно сервисной системы безопасности. «В период пандемии мы работали на удаленке, и защита информации в тот момент для нас была критическим моментом. Сегодня мы часто регистрируем попытки несанкционированного доступа к нашим ресурсам. В ближайших планах компании решить данную проблему, поэтому мы внимательно рассматриваем предложение «Ростелеком-Солар», тем более что у компании наработаны лучшие практики в сфере информационной безопасности»,— рассказал Сергей Очаковский.