ПОД КАПОТОМ ЦКБ

В Беларуси продолжает формироваться «армия» национальной кибербезопасности. В ее составе уже 28 специализированных центров кибербезопасности (ЦКБ), аттестованных Оперативно-аналитическим центром при Президенте. Это подразделения госорганов, в банках, промышленности, ИТ, связи.

О технологиях, на которых строится защита центра кибербезопасности, и о проникновениях, которые удалось пресечь, рассказал руководитель ЦКБ МТС Кирилл СУБОЧ. В мае 2024 года компания МТС аттестовала свой ЦКБ. Сегодня его специалисты защищают как собственную инфраструктуру, так и другие компании.

Тон тому, какие технологии следует использовать центрам кибербезопасности для выстраивания защиты от киберинцидентов, сегодня задает регулятор – Оперативно-аналитический центр при Президенте. Приказом ОАЦ № 130 определены минимальные требования для обеспечения защиты.

По словам Кирилла Субоча, еще на этапе подготовки к аттестации центра МТС определился, что пойдет по пути использования технических инструментов расширенной защиты для блокировки векторов проникновения угроз. Так, кроме обязательной для организации ЦКБ системы сбора и корреляции событий (SIEM), МТС для защиты выбрал платформу расширенного обнаружения и реагирования XDR, где SIEM является хоть и главным элементом, но не единственным. Помимо нее, в стек входят система сетевого анализа трафика, прокси-сервер, решения, направленные на защиту конечных точек, и др.

«Мы выбрали коробочное решение крупного российского вендора. Однако даже оно

в сложной инфраструктуре и при постоянно меняющемся поведении администраторов генерировало множество ложных срабатываний. Так стало очевидно, что даже для топ-продуктов требуются постоянная донастройка и формирование аналитической базы под конкретные задачи», – подчеркивает Кирилл Субоч.

За полтора года работы центр кибербезопасности МТС построил защитные «укрепления» для перекрытия всех основных векторов атак.

На периметре внедрено специализированное решение, которое позволяет автоматически анализировать исходящий трафик и выявлять потенциальные угрозы.

Для защиты от фишинговых атак действует комплексный механизм проверки почтового трафика, включающий актуальные технологии фильтрации и анализа. По данным ЦКБ МТС, именно такие решения позволяют значительно повысить уровень безопасности и блокировать угрозы, которые могут обходить стандартные средства защиты.

Интегрированная с SIEM платформа анализа угроз формирует предупреждения при попытках обращения к вредоносным ресурсам и обеспечивает своевременное реагирование на инциденты.

С помощью используемых технологий, по словам руководителя ЦКБ, предупреждено значительное количество целевых атак. Многие готовились за несколько месяцев.

Среди раскрытых тактик злоумышленников – отключение смены паролей через реестр, скрытый вывод списка активных учетных записей через инструменты вроде PowerShell, кража данных через создание теневых копий дисков и маскировка вредоносного ПО под процесс обновления браузера Google Chrome.

> ЦКБ МТС для защиты инфраструктуры использует платформу расширенного обнаружения и реагирования XDR, в которую, кроме системы сбора и корреляции событий (SIEM), входят система сетевого анализа трафика, прокси-сервер, решения, направленные на защиту конечных точек, и др.

Как говорит Кирилл Субоч, злоумышленники всегда действовали осторожно и уделяли внимание маскировке следов – подчищали журналы событий с помощью специализированных утилит.

> Тактики злоумышленников, которые раскрыл ЦКБ: отключение смены паролей через реестр, скрытый вывод списка активных учетных записей через инструменты вроде PowerShell, кража данных через создание теневых копий дисков и маскировка вредоносного ПО под процесс обновления браузера Google Chrome.

Эксперт по кибербезу отмечает два ключевых момента. Первый – сегодня выстраивание полноценной кибероборонbы возможно только с использованием комплексных и «тяжелых» решений. Это подтверждается и новыми регуляторными требованиями, которые вскоре обнародует ОАЦ.

Второй и главный тезис – покупка дорогостоящих инструментов теряет смысл без наведения базового порядка в инфраструктуре. Устранение слабых паролей, критических уязвимостей, внедрение сетевой сегментации – фундамент, без которого самый совершенный киберщит не может быть использован. ВС

Анастасия МАНУИЛОВА

Руководитель ЦКБ МТС Кирилл Субоч