Тем не менее, авторы постарались раскрыть ряд важных аспектов в данной области и сделать некоторые выводы, а именно:

• современный мир ставит перед всеми нами постоянно растущий ряд вызовов в области информационной безопасности, и от них нам нигде и никак не укрыться. Мы обязаны на них реагировать, а еще лучше, действовать с упреждением;

• число компьютерных атак растет и будет расти;

• имеется насущная необходимость в разработке и совершенствовании средств защиты информации: СЭ, СОВ (СОА), системах предотвращения вторжений, системах интеллектуального анализа и т.п.;

• российские программные и технические решения в области ИБ не только имеются, но и находятся высоком уровне, не уступая зарубежным аналогам (а порой и превосходя их);

• необходимо прививать и совершенствовать знания, умения и навыки в области ИБ – при чем для всех: от школьников и до высококвалифицированных специалистов в области ИБ. Это требует концентрации усилий всех субъектов образовательной среды: от школ до вузов и организаций дополнительного профессионального образования.

Список литературы

1. *Steve Morgan*. Cybersecurity labor crunch to hit 3.5 million unfilled jobs by 2021 [Электронный ресурс]. https://www.csoonline.com/article/3200024/cybersecurity-labor-crunch-to-hit-35-million-unfilled-jobs-by-2021.html
2. Актуальные киберугрозы: итоги 2019 г. https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2019
3. *Lance Spitzner*. Honeypots: Tracking Hackers. Addison Wesley, 2002.
4. Honeypots Solutions. https://web.archive.org/web/20090308063216/ http://www.tracking-hackers.com/solutions/

Васильев Николай Петрович *- канд. техн. наук, доцент, доцент кафедры КБ-1 «Защита информации» МИРЭА – Российского технологического университета (РТУ МИРЭА),*

Фефилов Александр Валерьевич *– старший специалист информационной безопасности АО «Перспективный мониторинг».*

И БЕЗОПАСНОСТЬ МОЖЕТ БЫТЬ НА АУТСОРСЕ

А.С. Филатов (Компания Tet)

Для обнаружения и устранения угроз в области информационной безопасности на предприятиях создаются центры управления безопасностью либо такие услуги предоставляются по подписке через аутсорсинг. Рассмотрены плюсы и минусы каждого из этих решений.

Ключевые слова: аутсорсинг, кибербезопасность, центры управления безопасностью, промышленные предприятия.

Утечки данных, заражение вредоносным ПО и кибератаки стали привычным явлением как для больших, так и для малых организаций по всему миру. Так, число инцидентов, связанных с программами-вымогателями, в производственном секторе увеличилось на 156% в период с первого квартала 2019 г. по первый квартал 2020 г.

Раньше ситуация была иная — компаниям промышленного сектора не нужно было подключать свои системы управления производством (Industrial control systems — ICS) к Internet. Это означало полную защиту от внешних угроз и не требовало ничего, кроме контроля за физическими процессами.

Теперь большинство компаний в том или ином виде имеют выходы в «большой» Internet, а значит и потребность в кибербезопасности выросла до уровня бизнеса из любой другой сферы. Для минимизации времени простоя, которое может быть вызвано атакой на предприятие, игрокам производственного сектора необходимо отслеживать и анализировать огромный объем данных в реальном времени.

Обнаружение и устранение угроз до того, как они вызовут какие-либо негативные последствия, — ежедневный приоритет для ИТ-команд. Однако, даже несмотря на усилия высококлассных специалистов по информационной безопасности, защититься от хакеров получается далеко не всегда.

Приходится принять тот факт, что добиться 100% безопасности невозможно ни при каких обстоятельствах. Можно лишь уменьшить риски и держать ситуацию под постоянным контролем. Многие ИТ-отделы достигают этих целей путем внедрения в свою деятельность центра управления безопасностью (security operations centre — SOC). Он может быть как частью самой компании, так и услугой по подписке.

Как можно управлять безопасностью?

Основная функция центра безопасности — круглосуточный мониторинг инфраструктуры с целью обнаружения, предотвращения или реагирования на киберугрозу, а затем проведение комплексного расследования. Команды SOC отвечают

за анализ и защиту акт вов организации, включая интеллектуальную собственность, персональные и критические бизнес-данные, системы компании и их целостность.

Для возможности максимально обезопасить периметр организации от разного типа киберугроз необходимо наблюдать буквально за каждым, даже мельчайшим происшествием в ИТ-инфраструктуре. Выявление аномалий в поведении «железа» и «софта» — непростая задача, требующая особых навыков и длительной подготовки. Любое из незамеченных отклонений от нормы может повлечь за собой серьезные последствия для репутации компании.

Профессионально организованный мониторинг — это эффективный инструмент оперативного реагирования на сбои в функционировании информационных систем и повышения производительности работы. Однако не всегда у компании есть ресурсы и экспертиза, чтобы создать такой центр самостоятельно.

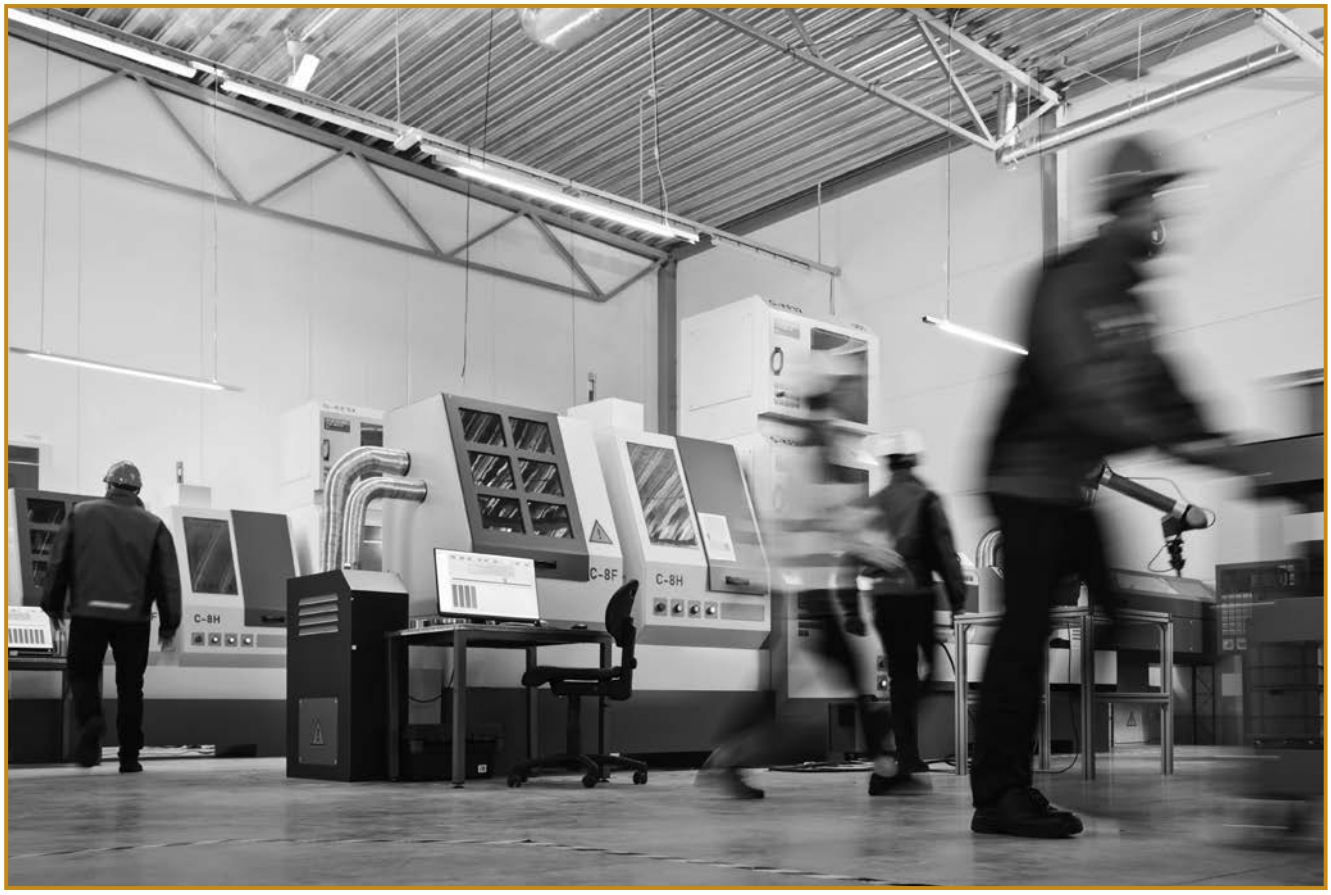
Доверить защиту третьим лицам — звучит опасно

Объем рынка глобальных операционных центров безопасности (SOC) оценивается в 34,73 млрд. долл. США в 2020 г. и, как ожидается, будет расти со среднегодовым темпом роста в 11,9% в течение прогнозируемого периода. Спрос на центры значительно увеличился из-за растущей потребности в мониторинге и анализе безопасности предприятия. Центры управления безопасностью укомплектованы аналитиками, инженерами и менеджерами, ответственными за обнаружение, анализ и эффективное реагирование на инциденты кибербезопасности.

Компания Tet уже более 3 лет предлагает услугу «центр управления безопасностью как сервис (SOC as a service)» своим клиентам в Латвии и на экспортных рынках, в том числе и России.

Услуга нацелена на сокращение затрат на эксплуатацию ИТ-систем и обеспечение их эффективного развития без дополнительных капитальных инвестиций. Число инструментов ИТ-безопасности растет едва ли ни каждый день, однако парадокс в том, что уследить за общей безопасностью организации не становится легче. Необходимо анализировать события каждого инструмента по отдельности, и только для этого нужен целый штат квалифицированных профильных специалистов. Вне зависимости от числа уже внедренных средств защиты, если своевременно не реагировать на возникающие угрозы, их эффективность стремится к нулю.

Для повышения эффективности принятия решений по реагированию на события, связанные с нарушением безопасности, рекомендуется использовать специализированные системы мониторинга, которые могут автоматизировать процесс сбора и анализа информации, поступающей от различных средств защиты. В западной терминологии такие системы мониторинга



обозначаются аббревиатурой SIEM (Security Information and Event Management). И такие решения обязательно входят в состав технических решений SOC.

Процесс мониторинга — это совокупность человеческих ресурсов, технических средств и организационных мер, направленных на решение задач, которые компания ставит перед мониторингом в процессе эксплуатации ИТ-инфраструктуры. Центр управления безопасностью как услуга на базе решений SIEM позволяет своевременно обнаруживать инциденты в периметре безопасности, централизованно собирать информацию по событиям из множества распределенных разнородных источников, обрабатывать ее и анализировать. Более того, провайдер решения берет на себя и контроль соответствия защищенности информационных систем корпоративным политикам и стандартам безопасности.

Как обеспечивается безопасность?

Основная задача SOC — защитить организацию от любого рода кибервмешательства в ее деятельность. Для этого используется целый ряд методов.

• *Расследование потенциальных инцидентов:* команды SOC получают большое число предупреждений, но не все они указывают на реальные атаки. Аналитики SOC несут ответственность за изучение потенциального инцидента, чтобы определить, действительно ли это реальная атака или ложное срабатывание.

• *Упорядочивание и приоритезация обнаруженных инцидентов*: не все инциденты безопасности одинаковы, а организация имеет ограниченные ресурсы для реагирования. После выявления нескольких инцидентов их необходимо приоритизировать, чтобы оптимизировать использование ресурсов и максимально снизить риски.

• *Координация реагирования на инциденты:* ответная реакция на инциденты требует взаимодействия с несколькими заинтересованными сторонами и использования множества различных инструментов. Аналитики SOC должны организовать этот процесс, чтобы гарантировать, что в совместной работе не возникнет ошибок, способных привести к отсрочке или неполному исправлению ситуации.

Главная проблема, с которой сталкиваются предприятия при самостоятельном внедрении центра управления безопасностью, — несоответствие возможностей команды центра с ее обязанностями. Провайдер SOC as a service может помочь нивелировать эту разницу, он:

• *наймет лучших специалистов:* отрасль кибербезопасности испытывает самый настоящий дефицит навыков, что затрудняет привлечение и удержание талантов, необходимых для защиты от киберугроз в штат. У провайдеров больше возможностей для найма высококлассных специалистов;

• *исключит ложные срабатывания:* в среднем SOC получает десятки тысяч предупреждений каждый день, но лишь небольшая часть связана с реальными угрозами. Аналитики SOC должны идентифицировать иголку в огромном стоге журналов и предупреждений на ежедневной основе, что отнимает значительно больше времени и ресурсов у специалистов с недостаточным опытом;

• *сведет к минимуму операционные последствия:* не все подозрительное в сети организации — это часть реальной атаки. Команды SOC должны блокировать только настоящие угрозы, не усложняя понапрасну жизнь самой компании;

• *быстро среагирует на атаку:* чем дольше злоумышленник имеет доступ к сети организации, тем больше убытков (материальных и нематериальных) понесет бизнес. Команды SOC должны быстро выявлять и сводить на нет атаки, чтобы минимизировать влияние на компанию;

• *соберет и отсортирует данные:* многие организации имеют сразу несколько решений для точечной безопасности. С одной стороны, это увеличивает защищенность каждого конкретного элемента инфраструктуры, но с другой — ухудшает «видимость» всей сети, а также снижает эффективность обнаружения инцидентов и реагирование на них. Провайдер возьмет на себя агрегирование данных с разных решений и обеспечит не только точечную защиту, но и надежную безопасность всего периметра.

Чем серьезнее бизнес относится к безопасности и конфиденциальности своих данных, тем больше доверия он заслуживает со стороны клиентов. SOC как услуга позволит получить глубокое представление о состоянии периметра организации и выявит места для улучшений, что позитивно отразится на репутации компании. Важно помнить, что потеря данных в случае кибератаки, скорее всего, повлечет за собой огромные издержки и упущенные доходы, в то время как «аренда» центра управления безопасностью ускорит переход бизнеса на более совершенную модель трат — OpEx, избавив его от еще одной строчки в списке капитальных расходов.

Филатов Артур Сергеевич *- руководитель бизнеса кибербезопасности Tet.*
E-mail: Arturs.Filatovs@tet.lv