Валерий ФИЛИН
технический директор
CITUM

Павел СТЕБЛЯНКО
генеральный директор
CITUM

Владимир СОЛОВЬЕВ
старший специалист отдела технических решений АО «ДиалогНаука»

АВТОМАТИЗАЦИЯ ПЕНТЕСТА — МИРОВОЙ ТРЕНД

ФАКТЫ О КИБЕРУГРОЗАХ И ВЫЗОВЫ

КИБЕРУГРОЗЫ СТАНОВЯТСЯ СЛОЖНЕЕ С КАЖДЫМ ГОДОМ

Угрозы ИТ-инфраструктуре организаций непрерывно усложняются и множатся. В своём отчёте по киберугрозам[1] от сентября 2020 года компания Microsoft отмечает, что за прошедший год злоумышленники серьёзно усилили свой инструментарий, всё чаще используя легитимное программное обеспечение (PsExec, netcat, powershell и т.д.) и применяя всё более сложные техники, препятствующие обнаружению угроз и в то же время позволяющие атаковать самые защищённые цели. (*«Threat actors have rapidly increased in sophistication over the past year, using techniques that make them harder to spot and that threaten even the savviest targets»*.)

УЩЕРБ ОТ КИБЕРАТАК РАСТЁТ С КАЖДЫМ ГОДОМ

По оценкам Accenture & Ponemon Institute[2], в 2018 году средний годовой ущерб от кибератак в финансовом секторе составил 13 млн долларов США в расчёте на одну организацию.

Потери российской экономики в 2019 году от действий кибермошенников составили около 2,5 трлн руб. Возможный ущерб от кибератак в 2020 году оценивается в 3,5–3,6 трлн руб.[3]

Средний ущерб от одного инцидента, связанного с критичными данными, оценивается в 3,86 млн долларов США[4].

ПЕРЕВОД СОТРУДНИКОВ НА УДАЛЁНКУ ПОРОЖДАЕТ ДОПОЛНИТЕЛЬНЫЕ КИБЕРРИСКИ

Вынужденный перевод сотрудников на удалённую работу в связи с пандемией привёл к существенным изменениям в инфраструктуре и правах доступа в большинстве организаций финансового сектора. Увеличение доли удалённых сотрудников закономерно приводит к повышению рисков ИБ: домашние компьютеры, используемые в качестве удалённых рабочих мест, хуже защищены и не подконтрольны организации. В то же время оценить дополнительные риски, связанные с предоставлением удалённого доступа, без пошагового моделирования сценариев атаки, сложно.

НЕХВАТКА КВАЛИФИЦИРОВАННЫХ КАДРОВ В ОБЛАСТИ ИБ

В соответствии с отчётом (ISC)[2] «Cybersecurity Workforce Study, 2020» количество незаполненных вакансий в области кибербезопасности в мире впервые в истории снизилось в 2020 году с отметки 4 млн, но всё ещё составляет непостижимые 3,1 млн[5].

АВТОМАТИЗАЦИЯ И ПРИОРИТИЗАЦИЯ ЗАДАЧ ИБ — ОТВЕТ НА ВЫЗОВЫ СЕГОДНЯШНЕГО ДНЯ

В условиях ограниченных ресурсов важно грамотно выстраивать приоритеты по задачам ИБ. Gartner подчёркивает необходимость фокусного анализа уязвимостей за счёт оценки их практической эксплуатируемости: *«Don't try to patch everything; focus on vulnerabilities that are actually exploitable»*. Риск-ориентированное управление уязвимостями и автоматизация анализа рисков безопасности внесены аналитиками Gartner в топ-10 проектов ИБ на 2020–2021 годы[6].

Для реализации фокусного подхода организации требуется выполнять регулярную практическую проверку защищённости. Золотым стандартом такой проверки является тестирование на проникновение (или пентест).

НЕПРЕРЫВНЫЙ ПЕНТЕСТ

Пентест — это трудоёмкая задача, поэтому традиционно выполняется 1–2 раза в год и зачастую в ограниченном масштабе. Сети современных организаций меняются существенно динамичнее, поэтому окно уязвимости между двумя последовательными пентестами является недопустимо долгим. Современный ландшафт угроз требует нового подхода — постоянное или непрерывное тестирование защищённости (рис. 1).

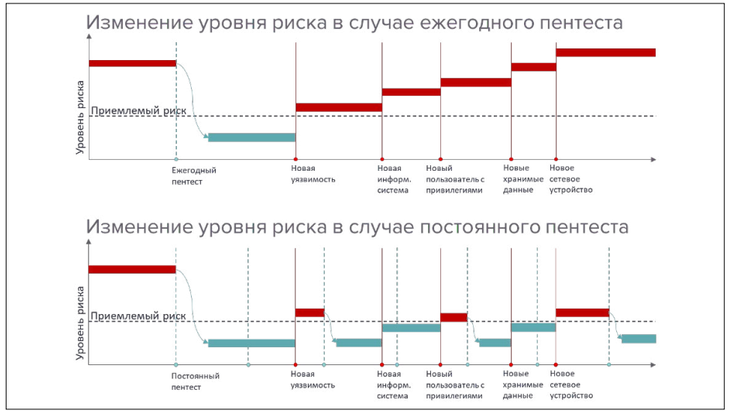

Рисунок 1. Изменение уровня риска в зависимости от периодичности пентеста

Можно выполнять непрерывный пентест вручную с помощью инструментов NPTT = Network Penetration Testing Tools (классификация Gartner). Однако найти высококвалифицированных пентестеров непросто, с учётом дефицита кадров на рынке. Ставка для таких сотрудников достаточно высока: не каждый позволит себе нанять в штат команду узкоспециализированных тестировщиков. И даже если в штате организации работает группа профессионалов-пентестеров, она не может гарантированно охватить всю ИТ-инфраструктуру для оценки возможных массовых векторов атак в полном масштабе и на регулярной основе. Злоумышленнику достаточно найти всего один рабочий вектор атаки, в то время как команде защитников важно обнаружить и ликвидировать все возможные векторы.

АВТОМАТИЗАЦИЯ ПЕНТЕСТА

Наиболее ценный результат даёт решение по автоматическому пентесту. Выполняя тестирование на проникновение с решением автоматизации, можно быть уверенными в том, что система найдёт все заложенные в неё векторы атак, с полным охватом «в ширину» и «в глубину», не испытывая влияния «человеческого фактора» — ничего не забывая и не упуская. При этом тестирование можно выполнять на регулярной основе: ежемесячно, еженедельно или ежедневно, — и в произвольном масштабе. Для выполнения автоматизированного теста на проникновение не требуется обладать квалификацией профессионального пентестера, что делает системы автоматизации доступными для широкого круга организаций.

Автоматизация пентеста даёт существенные преимущества:

- высокая скорость работы;
- снижение трудозатрат на оценку защищённости сети;
- снижение трудозатрат на оптимизацию защищённости сети;
- получение более быстрого результата и наглядного представления об уровне защищённости инфраструктуры по сравнению с ручным пентестом;
- быстрое и наглядное представление результатов от реализованных проектов ИБ, прозрачное обоснование для новых проектов;
- произвольный масштаб проверки за меньшее, чем при ручном пентесте, время;
- надёжный результат, не зависящий от человеческого фактора;
- анализ эффективности новых инструментов ИБ перед покупкой;
- экономия ресурсов за счёт мощной приоритизации уязвимостей и задач ИБ;
- обнаружение уязвимостей, действительно опасных для конкретной сети;
- возможность оперативного получения информации о новых векторах атак при любом изменении в ИТ-инфраструктуре;
- возможность инкрементального повышения защищённости за счёт внедрения исправлений или контрмер и мгновенной проверки результата, не дожидаясь очередного пентеста;
- возможность безопасной проверки эффективности внедрённых средств защиты, не дожидаясь реального инцидента;
- возможность регулярного тестирования эффективности процессов реагирования на инциденты, не дожидаясь реального инцидента;
- анализ защищённости без разглашения информации третьей стороне.

Всё это позволяет команде ИБ «держать руку на пульсе» рисков ИБ организации и оперативно реагировать в случае отклонений от приемлемого уровня. Автоматизация процесса анализа защищённости позволяет экономить значительные ресурсы ИТ/ИБ за счёт фокуса на обоснованно важных задачах ИБ и оптимизации уже внедрённых инструментов ИБ вместо внедрения новых.

PCYSYS PENTERA — УНИКАЛЬНОЕ РЕШЕНИЕ НА РЫНКЕ АВТОМАТИЗАЦИИ ПЕНТЕСТА

В настоящий момент единственным продуктом для автоматизации инфраструктурного пентеста является Pcysys PenTera. В подтверждение этой мысли Gartner включил Pcysys в отчёт Cool Vendors за 2020 год в категории Security Operations and Threat Intelligence. Цитата из отчёта: *«Pcysys provides an automated penetration testing solution, which is still unique in the security technology space. Pcysys' solution, PenTera, can be thought of as a human penetration tester offered as a technology. It is ideal for internal teams that are looking to replace manual penetration testing and increase the frequency of security testing»*. Запросить отчёт Gartner можно на сайте PCYSYS[7].

С 2019 года в России решение Pcysys PenTera широко применяется в проектах ведущими системными интеграторами и консультантами в сфере ИБ. Успешные проекты по автоматизации пентеста уже были реализованы в организациях различных размеров и отраслей экономики.

---

[1] https://blogs.microsoft.com/on-the-issues/2020/09/29/microsoft-digital-defense-report-cyber-threats/

[2] https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf.

[3] https://www.kommersant.ru/doc/4226302

[4] https://www.ibm.com/security/data-breach

[5] https://www.isc2.org/-/media/ISC2/Research/2020/Workforce-Study/ISC2ResearchDrivenWhitepaperFINAL.ashx

[6] https://www.gartner.com/smarterwithgartner/gartner-top-security-projects-for-2020–2021/

[7] https://go.pcysys.com/pcysys-named-2020-cool-vendor-in-security-operations-and-threat-intelligence