GROUP-IB

GROUP-IB × BANCA MEDIOLANUM

Обеспечение безопасности финансовых услуг в условиях сложной ИТ-инфраструктуры

ИСТОРИЯ УСПЕХА

О компании Banca Mediolanum

ОТРАСЛЬ

Банкинг и финансы

ГОД ОСНОВАНИЯ

1982

ГЕОГРАФИЯ

Офисы в Италии, Испании и Германии

Banca Mediolanum – итальянская компания, которая занимается банковской деятельностью, страхованием и управлением активами. У нее 3 офиса в разных странах Европы и более 6 тысяч сотрудников в штате. Банк Banca Mediolanum, основанный в 1982 году, на сегодняшний день входит в десятку крупнейших банков страны.

У Banca Mediolanum есть несколько дочерних компаний, в числе которых Mediolanum Group (поставщик финансовых услуг с головным офисом в Милане), а также другие финансовые организации с офисами в Испании и Германии. В общей сложности у Banca Mediolanum более миллиона клиентов в разных странах Европы; широкая география деятельности компании определяет потребность в передовых технологиях и инновационных решениях в области ИТ-безопасности.

Миссия компании

Banca Mediolanum трансформирует традиционные подходы, используемые на рынке банковских услуг. Компания не ограничивается техническими инновациями, руководствуясь в своих взаимоотношениях с клиентами идеей «свободы в выборе банковских услуг». В соответствии с этим принципом компания предлагает комплекс надежных и прозрачных финансовых решений, в основе которых лежат инновационные технологии, отличающиеся простотой в использовании.

Описание ситуации

Компании Banca Mediolanum необходимо эффективно управлять сложными ИТ-инфраструктурами в различных странах и бизнес-сегментах. Поэтому она использует широкий спектр сайтов, сервисов, мобильных приложений и прочих ресурсов для инвентаризации и защиты информации, а также управления информационными активами.

Сетевой периметр Banca Mediolanum постоянно расширяется. Сразу несколько подразделений компании занимаются обновлением инфраструктуры и созданием новых ресурсов, а это усложняет задачу команд ИТ и ИБ по поддержанию полной прозрачности всех доступных из сети ресурсов компании. Оценка уязвимостей, тестирование на проникновение и другие традиционные методы обеспечения безопасности имеют несомненную практическую ценность, однако применять их можно только в отношении известных ресурсов.

Основной проблемой для Banca Mediolanum было обнаружение скрытых угроз, то есть тех ресурсов, о существовании которых организация даже не догадывается. Поверхность атаки компании стремительно расширяется, поэтому необходимо регулярно отслеживать все доступные из сети ресурсы, управлять ими и обеспечивать их безопасность.

Почему выбрали Group-IB?

Выявление теневых ИТ и забытой инфраструктуры вручную требует больших затрат времени и усилий. Кроме того, необходимо учесть, что новые ресурсы развертываются в компании непрерывно, а значит для обеспечения полной прозрачности необходим регулярный мониторинг периметра.

Для упрощения и автоматизации этого процесса Banca Mediolanum воспользовалась AssetZero – решением Group-IB по мониторингу внешнего периметра с помощью данных киберразведки. Регулярно обновляя данные о внешнем периметре атаки, AssetZero позволяет Banca Mediolanum получить всестороннюю информацию о теневых ИТ и забытой инфраструктуре.

Также AssetZero каталогизирует все доступные из сети ресурсы, отслеживает уязвимости, оценивает уровень риска для каждого ресурса и приоритизирует задачи по устранению выявленных проблем. Благодаря обнаружению и категоризации уязвимостей сотрудники подразделения информационной безопасности Banca Mediolanum получили возможность сосредоточить усилия на решении самых срочных задач. По мере устранения проблем соответствующие тикеты на панели инструментов AssetZero помечаются как решенные, при этом оценка рисков обновляется в режиме реального времени.

Благодаря автоматизированному и непрерывному сканированию и обнаружению ресурсов AssetZero позволяет значительно сократить время, необходимое командам ИТ и ИБ для поиска ресурсов. Сотрудники, отвечающие за безопасность, получают возможность сосредоточиться на устранении уязвимостей с наибольшим уровнем риска, а это позволяет таким компаниям, как Banca Mediolanum, получать отличные результаты, затрачивая минимум усилий. Таким образом, внедрение AssetZero гарантирует компании возврат инвестиций.

Об AssetZero

1 Решение Group-IB

Система AssetZero для защиты внешнего периметра от кибератак и управления рисками

AssetZero представляет собой основанное на данных киберразведки SaaS-решение, позволяющее определять и анализировать поверхность атаки сложных инфраструктур, а также управлять ею при помощи единого простого интерфейса. Решение обеспечивает полную видимость доступных извне ресурсов организации, включая теневые ИТ и забытую инфраструктуру, и выявляет наиболее уязвимые из них. В зависимости от присвоенного уровня риска, решение приоритизирует необходимые действия по устранению последствий.

В отличие от других продуктов для управления внешней поверхностью атаки, AssetZero выходит за рамки базовой инвентаризации ресурсов и дает доступ к уникальным данным из признанной международными агентствами системы Group-IB Threat Intelligence & Attribution. Эта информация помогает партнерам сопоставлять ресурсы клиентов с упоминаниями на хакерских форумах, утечками пользовательских данных, активностью ботнетов, результатами исследований вредоносных программ и сетевыми коммуникациями серверов управления злоумышленников. Клиентам отправляются уведомления, связанные с важными объектами и критическими уязвимостями.

По мере устранения проблем соответствующие тикеты удаляются с панели инструментов, однако сохраняются в системе, чтобы партнеры могли отслеживать изменения в режиме реального времени. AssetZero также дает партнерам возможность сравнивать уровни защищённости клиентов с другими компаниями в том же регионе или в той же отрасли. Расширенный функционал по созданию отчетов позволяет легко извлекать данные из AssetZero и демонстрировать результаты его работы заинтересованным сторонам.

Результаты для бизнеса

2 Развертывание AssetZero также позволило Banca Mediolanum существенно повысить эффективность коммуникаций между командами, особенно – между ИТ и ИБ специалистами. Более того, технические подразделения стали более эффективно коммуницировать с бизнес-подразделениями компании.

Внедрение AssetZero позволило Banca Mediolanum добиться целого ряда значимых измеримых результатов. За счет повышения прозрачности всех доступных из сети ресурсов, а также получения информации о потенциальных уязвимостях компании удалось значительно снизить среднее время устранения уязвимости. Помимо этого, компания сэкономила сотни человеко-часов, которые пришлось бы потратить сотрудникам подразделений по ИТ, ИБ, управлению рисками и внутреннему контролю на поиск теневых информационных технологий и инвентаризацию ресурсов.

Например, внедрение AssetZero позволило ИБ-департаменту соотнести инфраструктуру банка с определенными регионами, представив информацию в понятной операционным подразделениям форме. Это помогло повысить интерес сотрудников к информационной безопасности и увеличить поддержку и бюджеты ИБ-подразделений. В итоге повышение уровня взаимопонимания позволило объединить усилия подразделений бизнеса, ИТ и ИБ, добиться более эффективного кросс-функционального сотрудничества и существенно повысить уровень защищенности Banca Mediolanum.

FAVIO GIANNOTTI, директор Banca Mediolanum по информационной безопасности

Благодаря AssetZero Banca Mediolanum удалось в кратчайшие сроки значительно повысить уровень своей защищенности. Это решение помогло нашей компании обнаружить доступные из сети ресурсы и приоритизировать меры по устранению угроз. Тем самым AssetZero позволил команде информационной безопасности сэкономить время, а компании – избежать лишних расходов за счет перераспределения ресурсов команды на самые важные задачи. Помимо этого нам удалось повысить эффективность взаимодействия между подразделениями, что способствует увеличению уровня безопасности всей организации

GROUP-IB

ПРЕДОТВРАЩАЕМ И РАССЛЕДУЕМ КИБЕРПРЕСТУПЛЕНИЯ С 2003 ГОДА

70 000+
часов реагирования

1 300+
успешных расследований по всему миру

Group-IB — одна из ведущих международных компаний по детектированию и предотвращению кибератак, выявлению фрода и защиты интеллектуальной собственности в сети.

По версии Gartner, IDC и Forrester, Group-IB является одним из ключевых поставщиков Threat Intelligence в мире, а в базе компании хранится 100 000+ профайлов киберпреступников.

Клиентами Group-IB являются крупнейшие банки и финансовые организации, промышленные и транспортные корпорации, ИТ и телеком провайдеры, ритейл и FMCG компании в 60 странах мира.

group-ib.ru/assetzero
assetzero@group-ib.com

Узнайте больше
о решении AssetZero