Astrum (ООО «Аструм»)
125040, г. Москва, ул. Нижняя, д. 14, стр. 1
Телефон: +7 (495) 98-89-105
Email: info@astrum-it.ru
Сайт: www.astrum-it.ru

Повышение осведомленности персонала с использованием методов фишинговых атак

В настоящее время многие организации все чаще подвергаются целенаправленным хакерским атакам. При этом использование современных многоуровневых систем защиты информации не дает 100%-го эффекта, так как основной вектор атак – это сотрудники. Используя методы социальной инженерии, злоумышленники, основываясь на особенностях психологии людей, побуждают пользователей выполнить определенные действия, которые в результате приводят к получению доступа к конфиденциальной информации, паролям, банковским данным и другим защищенным системам.

Одной из самых часто применяемых и эффективных форм атак с использованием методов социальной инженерии – это *фишинг* (англ. phishing, от fishing — рыбная ловля, выуживание). Целью фишинга является получение доступа к конфиденциальным данным пользователей, либо заражение персональных компьютеров с целью укрепления в информационной инфраструктуре и последующее полномасштабное вторжения в корпоративную сеть. *Фишинг-атака реализуется посредством рассылки тщательно разработанных электронных писем с вредоносным вложением или со ссылкой на вредоносный сайт (Приложение №1 – примеры фишинговых сообщений).*

Направленный фишинг стал самым распространенным типом таргетированной атаки по одной простой причине: эта техника по-настоящему работает, вводя в заблуждение даже тех пользователей, которые серьезно подходят к вопросам безопасности. Успешная атака создает для хакеров опорный пункт для проникновения в корпоративную сеть компании.

Новостные факты:

Хакеры украли у банков почти 2 млрд руб. с помощью «писем от ЦБ»
http://www.rbc.ru/finances/17/03/2016/56e97c089a794797e5b8e6b3

Хакеры замаскировали атаку на российские банки под уведомление от ЦБ РФ
http://www.banki.ru/news/lenta/?id=8784952&r1=rss&r2=common&r3=news

Astrum (ООО «Аструм»)
125040, г. Москва, ул. Нижняя, д. 14, стр. 1
Телефон: +7 (495) 98-89-105
Email: info@astrum-it.ru
Сайт: www.astrum-it.ru

Безопасность системы равна безопасности самого слабого звена – гласит основной принцип информационной безопасности. Это означает, например, что в случае если из тысячи пользователей, **хотя бы один** сотрудник откроет фишинговое сообщение, то защищенность других пользователей и информационных систем не имеет значения – этот рубеж защиты окажется быстро и легко преодолим через неподготовленного сотрудника. Поэтому, какую бы основательную техническую систему защиты вы не строили, про главное и в то же самое время очень слабое звено системы защиты – пользователей, и их обучение, забывать не стоит. Периодические инструктажи и информационные рассылки являются важной составляющей обучения персонала, но, как показывает практика, их эффективность значительно ниже, нежели обучение сотрудников на собственных ошибках.

Мы предлагаем

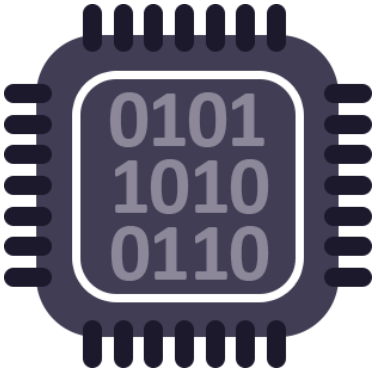
Компания Astrum предлагает услугу по «Повышению осведомленности персонала с использованием методов фишинговых атак». В рамках данной услуги мы развернем специализированную систему для организации фишинговых рассылок (с вложениями различных форматов и ссылками перехода) на электронные адреса сотрудников, подготовим сценарии проверки, разработаем уникальные шаблоны писем, проведем оценку результатов, разработку материалов для повышения уровня осведомленности персонала в вопросах информационной безопасности.

Данная услуга разделяется на организационную и техническую часть.

В рамках организационной части мы делаем:

- ✓ Сбор и анализ необходимой информации в зависимости от установленной зоны проведения работ;
- ✓ Разработку плана мероприятий по проведению проверки;
- ✓ Разработку стратегии атаки и сценариев рассылок;
- ✓ Разработку уникальных фишинговых писем (в зависимости от специфики вашей деятельности);
- ✓ Анализ статистики, разработку отчета и предоставление рекомендаций;
- ✓ Разработку обучающих материалов (в случае необходимости).

В рамках технической части мы делаем:



- ✓ Внедрение специализированной системы для организации «фишинговых рассылок» (на базе open-source решения);
- ✓ Адаптацию и настройку специализированной системы для организации «фишинговых рассылок» в соответствии с техническими особенностями вашей ИТ-инфраструктуры
- ✓ Тестирование «фишинговой рассылки» на фокус-группе пользователей.

Логическая схема работы системы для организации «фишинговых рассылок» представлена в Приложении №2.

Услуга по «Повышению осведомленности персонала с использованием методов фишинговых атак» максимально приближена к реальной модели фишинговой атаки, и призвана проверить готовность ваших сотрудников к подобного рода нападениям (через электронные письма), повысить бдительность пользователей при работе с корпоративными информационными ресурсами, повысить осведомленность сотрудников в вопросах корпоративной и личной информационной безопасности.

Так же данная услуга позволит выстроить непрерывный процесс повышения осведомленности персонала с возможностью оценки результатов и предоставления необходимых показателей руководству.

Выгода для вас

Недопущение непредвиденных финансовых затрат за счет снижения рисков утечки сведений ограниченного распространения, репутационных рисков, а также негативного влияния на бизнес-процессы организации.

КОНТАКТЫ

Лавров Алексей
Тел.: +7 (495) 98-89-105
E-mail: a.lavrov@astrum-it.ru

Михеев Константин
Тел.: +7 (495) 98-89-105
E-mail: mkm@astrum-it.ru

Astrum (ООО «Аструм»)
125040, г. Москва, ул. Нижняя, д. 14, стр. 1
Телефон: +7 (495) 98-89-105
Email: info@astrum-it.ru
Сайт: www.astrum-it.ru

Приложение №1

Примеры фишинговых писем

Пример №1:

Главному бухгалтеру:

От: *нейтральный адрес, типа %surname%%birthyear%@mail.ru*

Тема письма: *FWD акт сверки*

Текст письма: *Добрый день, ФИО. Согласно предварительной договоренности высылаю акт сверки.*

Приложение: *Акт сверки ООО «название вымышленной компании»**.xls***

Пример №2:

На общий адрес или Секретарю:

От: *info@msk.arbitr.ru (поддельный адрес)*

Тема письма: *Исковое заявление о взыскании долга*

В Арбитражный суд г. Москвы подано исковое заявление №23401-16 о взыскании долга с ООО «Название вымышленной фирмы», ЕГРЮЛ: XXXXXXXXXXXX, ИНН: XXXXXXXXXX, Юридический адрес:..., свидетельство о регистрации: XXXXXX на основании искового заявления контрагента по взысканию задолженности за оказанные услуги.

Исковые требования:

В соответствии со ст. 395 ГК РФ за пользование чужими денежными средствами вследствие их неправомерного удержания, уклонения от их возврата, иной просрочки в их уплате либо неосновательного получения или сбережения за счет другого лица подлежат уплате проценты на сумму этих средств.

Приложение: *судебное решение 23401-16**.docx***

Пример №3:

Сбербанк России

Уважаемый Клиент!
Кредитный отдел Сбербанка Росси уведомляет Вас о том, что на ваше имя 20.09.2015 был оформлен потребительский кредит через наш онлайн банкинг (xxx//online.sberbank.ru) на сумму 680 000 рублей.
На данный момент задолженность не погашена. На 01.11.2015 ваш долг составляет 633 773 рублей с учетом пени (0.7% сутки).
В связи с этим, на ваше имя Сбербанк России был составлен судебный иск.

Ознакомьтесь с документами:

Договор займа.rar
Судебный иск.rar

С Уважением.
Сбербанк России

Astrum (ООО «Аструм»)
125040, г. Москва, ул. Нижняя, д. 14, стр. 1
Телефон: +7 (495) 98-89-105
Email: info@astrum-it.ru
Сайт: www.astrum-it.ru

Приложение №2

Логическая схема работы системы для организации «фишинговых рассылок»