Innostage: 77% организаций в России недостаточно защищены от взлома

Тематика: **IT и телекоммуникации**
Статьи и исследования

г. Москва

Дата публикации: 28.12.2022

Дата мероприятия / события: 28.12.2022

Группа анализа защищенности компании Innostage провела тестирование на проникновение (пентест) в российских компаниях и подводит промежуточные итоги. Целью пентеста являлось получение максимально возможных привилегий или выполнение нелегитимного действия по отношению к ИТ-инфраструктуре организации.

В 77% организаций специалистам удалось получить административный доступ к критичным объектам или чувствительной информации, находясь за пределами внешнего периметра.

В рамках внутренних пентестов (изнутри ИТ-инфраструктуры) удалось скомпрометировать доменную инфраструктуру 91% организаций-участников. Рекордная по скорости компрометация заняла всего 3 часа.

В процессе проведения фишинговых рассылок у каждой второй компании более 10% сотрудников отреагировали на письмо и выполнили соответствующие действия: выслали ответное письмо с запрашиваемой информацией, запустили вредоносное ПО, ввели учетные данные. В одной из компаний этот показатель обратной связи достиг 34%, что явно говорит о недостатке осведомленности сотрудников об атаках с применением социальной инженерии.

«Полученные нами результаты говорят, что в 61,5% организаций уровень защищенности недостаточный для противодействия внешнему нарушителю и в 91% – недостаточный для защиты от внутреннего нарушителя», ?
рассказывает **Александр Борисов, руководитель направления анализа защищенности Innostage.**

Аналитики Innostage отмечают, что основными уязвимостями, используемыми при преодолении сетевого периметра, являются уязвимости веб-приложений и использование слабых паролей для внешних сетевых сервисов.

Использование предсказуемых паролей пользователями не только дает возможность внешнему удаленному злоумышленнику преодолеть сетевой периметр организации, но и делает уязвимым внутреннюю ИТ-инфраструктуру. Зачастую парольная политика в компаниях существует только на бумаге. Дополнительные средства, которые могли бы контролировать ее исполнение, организации не применяли. Используемые компаниями стандартные средства контроля не могли обеспечить достойное соблюдение требований к длине или сложности пароля. В сервисах, не поддерживающих централизованное управление парольной политикой, контроль учетных данных отсутствовал полностью.

Кроме использования словарных паролей, аналитики Innostage выделяют избыточные и небезопасные протоколы. При этом в большинстве случаев они не являлись технической необходимостью, представляя собой настройку «по умолчанию».

Уязвимости, эксплуатация которых способствовала успешному проведению атак в процессе внутреннего тестирования, и процентное соотношение частоты использования в ходе проведения работ специалистами Innostage представлены ниже:
· использование предсказуемых паролей (87%),
· применение небезопасных протоколов (78%),
· небезопасная конфигурация учетных записей в AD (39%),
· небезопасная конфигурация хостов в домене (39%),
· отсутствие принудительной подписи протоколов (34%),

· небезопасное хранение паролей (30%),
· отсутствие разграничения доступа к информации, размещенной в общих сетевых папках (17%),
· небезопасная конфигурация AD CS (13%).

По итогам проведенных работ организации получили рекомендации по повышению уровня защищенности с учетом особенностей импортозамещения.

Innostage — российская ИТ-компания, разработчик и интегратор сервисов и решений в области цифровой безопасности.

Синергия уникальных ИТ-технологий и экспертизы команды Innostage позволяют обеспечивать цифровую устойчивость бизнеса лидеров рынка, имеющих высочайшие требования к уровню информационной безопасности.

Ключевые направления:
- Консалтинг
- Информационная безопасность
- Системная интеграция
- Внедрение средств защиты информации
- Безопасность АСУ ТП
- Разработка бизнес-решений и ПО
- Построение и развитие ИТ-инфраструктуры

Innostage оказывает услуги по аудиту и формированию дорожных карт комплексного импортозамещения цифровых сервисов и ИТ-инфраструктуры.

Также на базе Innostage функционирует профессиональный центр противодействия киберугрозам Innostage CyberART, осуществляющий комплексный подход к противодействию цифровых угроз за счет превентивного анализа рисков и управления уязвимостями, выявления попыток атак на раннем этапе и немедленного реагирования на них с целью полного нивелирования возможных последствий и устранения причин возникновения инцидентов. Является центром ГосСОПКА.