Необходимость ликвидации статических паролей

Майк Эдвардс
Директор по продажам
Cryptocard Europe

Область применения

В мире более 600 миллионов персональных компьютеров,

НО

90% из них до сих пор используют статические пароли,

ПОЭТОМУ

здесь есть БОЛЬШИЕ перспективы.

Область применения

В мире более 600 миллионов персональных компьютеров,

НО

90% из них до сих пор используют статические пароли,

ПОЭТОМУ

здесь есть БОЛЬШИЕ перспективы.

СТАТИЧЕСКИЕ ПАРОЛИ

Что не так со статическими паролями ?

Они являются СЛАБЫМ звеном в системе безопасности.

ПОЧЕМУ ЕСТЬ СЕРЬЕЗНЫЙ РИСК

...что пароль может быть легко предсказуем, взломан или даже виден

Потому что…

...обычно они простые, разделяемые с коллегами, а иногда даже записаны на стикерах, приклеенные на мониторах.

ПОЧЕМУ ОНИ НЕ БЕЗОПАСНЫ

КТО ГОВОРИТ, ЧТО ЭТО ПРОБЛЕМА

“ Управление паролем входит в «Десятку» уязвимостей в безопасности, с которыми сталкиваются компании сегодня. ”

По словам: SANS Institute
Gartner
FBI

ПУГАЮЩИЕ ФАКТЫ

По данным последних исследований, LC4 (программа взлома паролей) угадывает половину случайных, программно-сгенерированных, “сложных” паролей ……..

МЕНЕЕ ЧЕМ ЗА 3 МИНУТЫ!

The SANS Institute

НИКТО НЕ ЗАЩИЩЕН!

MICROSOFT ВЗЛОМАН ! КОД УКРАДЕН!

“…. Хакеры воспользовались украденными паролями с целью проникновения в секретные зоны сети и начали скачивать служебные документы”

T. Bridis and R Buckman
The Wall Street Journal Online

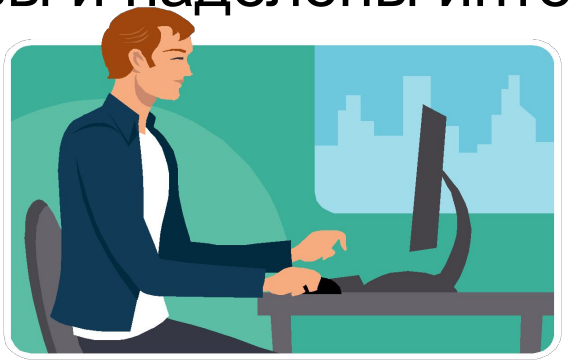
ВНУТРИСЕТЕВАЯ УГРОЗА

«БОЛЕЕ 50% сетевых атак
были запущены внутри сети.»

Gartner

ОПАСНОСТЬ ИЗВНЕ

Угроза реальна и непрерывно возрастает, потому что “электронная преступность” это уже не просто вредоносные действия безмозглых мальчиков. Преступники хорошо организованны, укомплектованы, находчивы и наделены интеллектом.



ФИШИНГ-АТАКИ

citi

Dear CitiBank customer,

Recently there have been a large number of identity theft attempts targeting CitiBank customers. In order to safeguard your account, we require that you confirm your banking details.

This process is mandatory, and if not completed within the nearest time your account may be subject to temporary suspension.

To securely confirm your Citibank account details please go to:

https://web.da-us.citibank.com/signin/scripts/login/user_setup.jsp

Thank you for your prompt attention to this matter and thank you for using CitiBank!

Citi® Identity Theft Solutions

Do not reply to this email as it is an unmonitored alias

A member of citigroup

Copyright © 2004 Citicorp

ТАК ЗАЧЕМ ЖЕ СТАТИЧЕСКИЕ ПАРОЛИ?

Потому что IT менеджеры верят, что они “БЕСПЛАТНЫЕ”

НАСТОЯЩАЯ ЦЕНА “БЕСПЛАТНЫХ” ПАРОЛЕЙ

Рассмотрим 2 факта….

“Обычно компания численностью 2,500 пользователей тратит только около 500,000$ в год на техническую поддержку”

Gartner

“Более 30% обращений к системному администратору связаны с паролями”

GIGA Group

СТАТИЧЕСКИЕ ПАРОЛИ- РОСКОШЬ!

Таким образом, стоимость использования статических паролей на этом примере составляет….

Приблизительно 60$ на пользователя…КАЖДЫЙ ГОД

Они какие угодно, но не БЕСПЛАТНЫЕ!

ЧТО СТИМУЛИРУЕТ РЫНОК

НЕОБХОДИМОСТЬ СОБЛЮДЕНИЯ ЗАКОНОВ

Организации понимают, что находится под угрозой, и обращаются за подтверждением в государственные и наблюдающие организации, устанавливающие строгие стандарты и личную ответственность представителей компаний по законам о защите информации:

- **Закон по обеспечению доступности и подотчетности в мед.страх. (HIPAA)**
- **Закон по борьбе с корпоративным и бухгалтерским мошенничеством (SOX)**
- **Закон о защите частной фин. информации (GLB)**
- **Закон, регулирующий электронную и цифровую подпись (21 CFR Part 11)**
- **Приложение 11 закона об автоматизированных системах**
- **Директива о защите данных (95/46/EU)**
- **Международное соглашение (Basel II)**
- **Японская директива о защите информации**

Официальная позиция..

Компании должны быть в состоянии доказать, что пользователи, которым предоставляется доступ к их данным, являются теми за кого себя выдают...

Использование статических паролей может привести к административному преследованию.

ИДЕАЛЬНЫЙ ПАРОЛЬ :

Должен быть сложным

Никогда не использоваться дважды

Принадлежать одному пользователю

Работать на любой точке доступа

Легкий в эксплуатации

Не требующий управления в отличии от статического

Менее затратным, чем статический

ДВУХФАКТОРНАЯ АУТЕНТИФИКАЦИЯ

Фактор 1: Что-то, что принадлежит ТОЛЬКО ВАМ (Ваш токен)

Генерирует уникальный пароль

Фактор 2: Что-то, что знаете ТОЛЬКО ВЫ (Ваш PIN)

В сочетание с кодом создает единоразовый пароль (One-time Password)

+

ПРЕИМУЩЕСТВА 2FA

Пароль не может быть совместным, украденным, забытым или записанным.

Если токен потерян или украден , он бесполезен без PIN-кода

В отличие от украденного пароля, пропажа токена обнаружится немедленно

Тех.поддержка избавится от обязанностей по поддержке паролей

Вы усилите контроль доступа к Вашим сетевым ресурсам

ПОЧЕМУ ИМЕННО CRYPTOCARD

Уникальные возможности для продаж

Абсолютная независимость

Многоформатность отгрузки

Мультиплатформенность

Широкий ассортимент токенов

Самостоятельная инициализация

Аппаратные токены – единоразовая покупка

Наиболее надежные пароли (8 character base 64)

АБСОЛЮТНАЯ НЕЗАВИСИМОСТЬ

Systems	Databases	Username	Web /App	SSL-VPN	Firewall
Microsoft Windows XP 2000 Pro SP4 2003 Server SP1 Mac OS X 10.3.x Panther OS X 10.4.x Tiger RedHat Ent. 3.x-4.x SuSE Ent. 9.x	POWERED BY MySQL 4.0.2, 4.1.x Microsoft SQL Server 2000 Enterprise Edition Enterprise 2000 (SP4) ORACLE 9i, 10g	Microsoft Active Directory OpenLDAP Mac Open Directory	Apache Web Sever 1.3-2.x Microsoft IIS 6.x CITRIX Citrix Web 4.0 Microsoft Office Outlook Web Access Exchange 2003 SP1	WatchGuard Firebox SSL Core Cisco Systems 3000 Concentrator NORTEL Connectivit y CITRIX Access Gateway Checkpoint Juniper Sonic Wall F-Secure	Borderware Checkpoint Netscreen Sonicwall Watchguard Cisco Systems pix

МНОГОФОРМАТНОСТЬ ОТГРУЗКИ

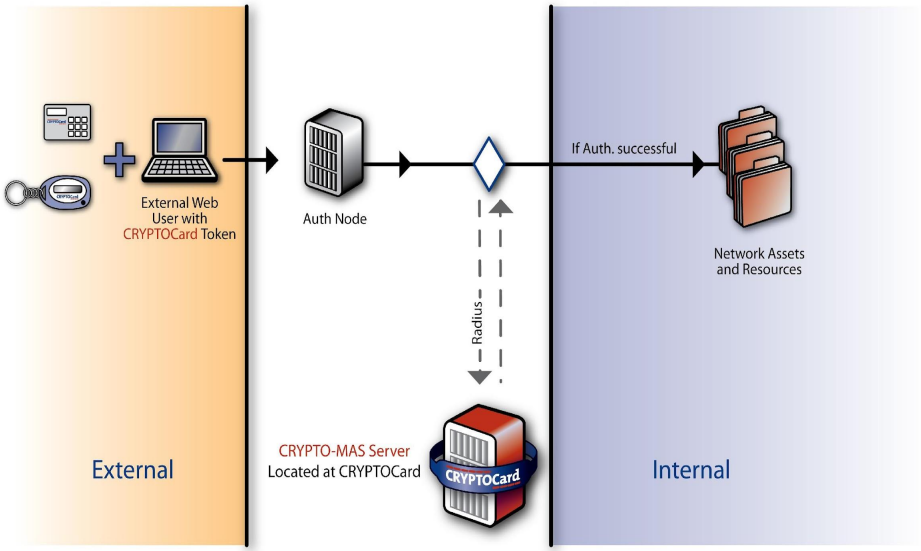
CRYPTO-MAS
Служба Управления Аутентификацией для организаций, которые не обладают опытом и не испытывают желания строить собственную структуру внутренней аутентификации.

CRYPTO-Shield
Готовая к внедрению Инфраструктура Аутентификации, включающая в себе возможности инициализации, управления и т. д.

AuthEngine
Основное ядро Механизма Аутентификации в виде закрытого кода для дальнейшего внедрения в уже существующие приложения, предназначенное для разработчиков.

MAS Служба Управления Аутентификацией

1. Управляемая двухфакторная аутентификация
2. Небольшие первоначальные затраты
3. Быстрое внедрение
4. Не требуется специальной квалификации
5. Недорогая ежемесячная абонентская плата



An Auth Node is a system or application within the network that challenges the user to authenticate and communicates with the CRYPTO-MAS Server . Examples include: IPSEC or SSL VPN, Firewall, Web Application, Citrix Gateway, Web email (eg. OWA), Web Portal, ISA, etc.

= Authentication Request

CRYPTO-SHIELD

CRYPTO-Server Интеграция с LDAP/AD

Хранение информации о токенах в MySQL или Oracle

Взаимодействие с приложениями по протоколам RADIUS,HTTP,HTTPS or CAP

Возможность репликации и восстановления при сбоях

Версии для Windows, Linux or Mac

CRYPTO-Console Управление GUI

Просмотр каталогов

Управление токенами

CRYPTO-Logon Обеспечивает возможность авторизации для ПК и доменов

CRYPTO-Web Обеспечивает возможность защиты Web-страниц и порталов

AUTH ENGINE

Встраиваемое в существующую бизнес-среду решение по аутентификации с использованием токенов

Взаимодействует, замещает или дополняет существующие методы аутентификации, в том числе использующие статические пароли.

Интегрируется с существующими системами инициализации, обработки и выполнения заказов, выставления счетов, технической поддержки, бухгалтерской отчетности и др.

Применяется в существующей инфраструктуре:

- Баз данных
- Приложений
- Производства

МНОГОПЛАТФОРМЕННОСТЬ

Достоинство многоплатформенности серверного программного обеспечения не только в поддержке всех основных операционных систем.

Это возможность построения пользовательской среды на базе единичных решений, корпоративной сети, объединением их в единое целое.

Удобство оценят корпорации, в которых тенденция роста основана на присоединении новых филиалов. Они всегда могут уверены, что выбранное ими решение по двухфакторной аутентификации легко внедряемо.

ШИРОКИЙ АССОРТИМЕНТ ТОКЕНОВ

Различные типы пользователей…

Сетевые пользователи (LAN)

Удаленные пользователи

Надомные работники

Контактные специалисты

Технические специалисты

Финансовые служащие

Кадровые сотрудники

Существует разные технологии и уровни безопасности.

Хорошие новости в том, что….

У нас есть подходящие токены для всех.

САМОСТОЯТЕЛЬНАЯ ИНИЦИАЛИЗАЦИЯ

Мы позволяем конечным пользователям самостоятельно инициализировать их аппаратные токены.

Это предотвращает возможность доступа третьей стороны к Вашей частной сети.

Задайте себе вопрос……..“Это в ваших правилах делится с кем-либо своим индивидуальным ключом ?”

Если нет, то есть только одно решение, которое можно купить!

ТОКЕН – ЕДИНОРАЗОВАЯ ПОКУПКА

Конкуренты изобрели один из лучших способов финансового мошенничества, который только можно было придумать!

Они заставляют Вас покупать токены снова и снова.

Это не только очень дорогой вариант для пользователей, но и неудобство, так как вы постоянно вынуждены заново внедрять токены.

С Cryptocard Вы покупаете однажды и внедряете один раз и навсегда.

НАИБОЛЕЕ НАДЕЖНЫЕ ПАРОЛИ

Основные конкуренты могут генерировать только шестизначные цифровые пароли

Другие способны сочетать в паролях цифры и алфавит (0-9 plus A-F)

Время на подбор пароля методом перебора

Длина пароля	Только цифры	Алфавит и цифры 0-9 плюс A-F	Алфавит и цифры Base64 0-9, a-z, A-Z Специальные символы
4	Несколько секунд	Несколько секунд	Несколько секунд
6	< 60 секунд	Около 1 минуты	Около 15 минут
8	Приблизительно 58 часов	Приблизительно 1 год	Приблизительно 7 лет
10	Приблизительно 5 лет	Приблизительно 2,000 лет	Приблизительно 26,984 лет

CRYPTOCARD в РОССИИ

Мы получаем Сертификат ФСТЭК

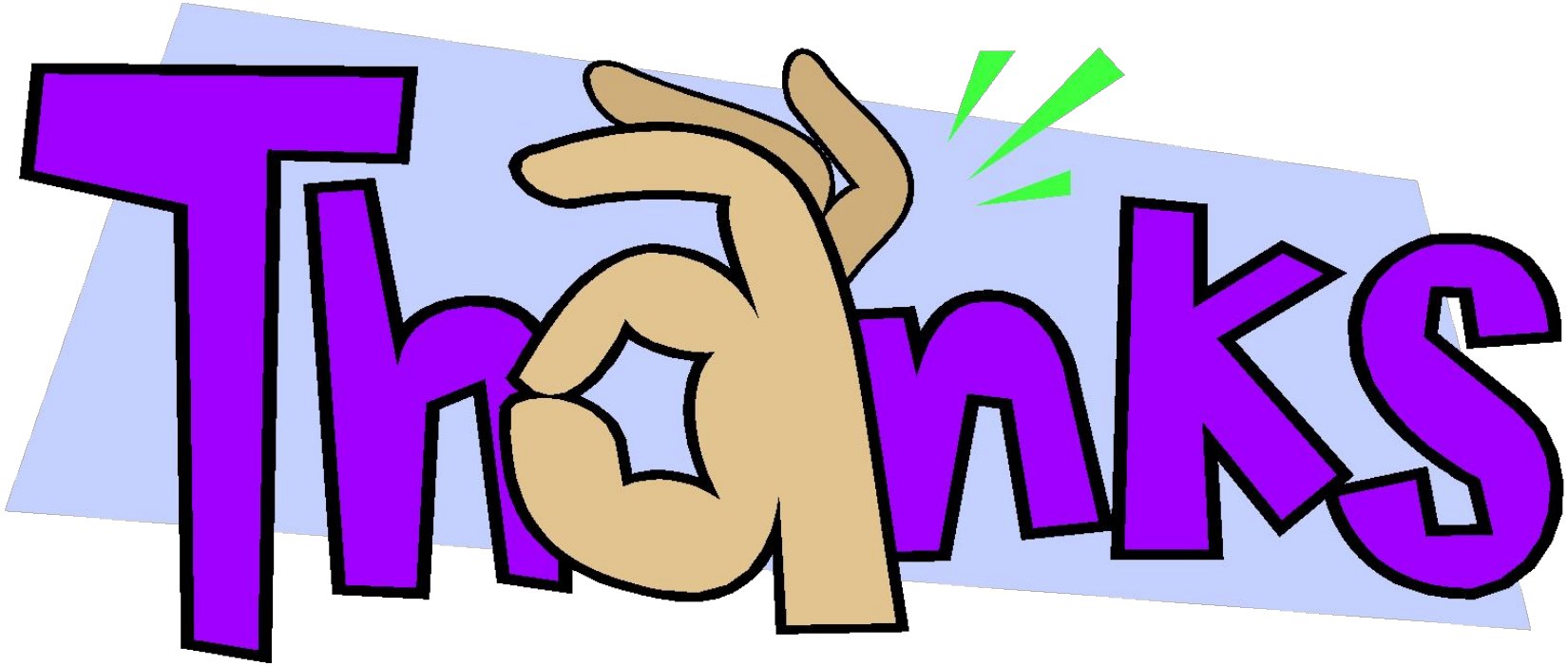
Наш опытный дистрибьютор – Сетевые решения

Мы готовы …….. К СОТРУДНИЧЕСТВУ

ЗАПОМНИТЕ, ПОЖАЛУЙСТА

Чем Лучше Продукт

по Лучшей Цене,

тем Лучше Результат

СПАСИБО ЗА ВНИМАНИЕ