Sua organização está preparada para lidar com **ATAQUES CIBERNÉTICOS?**

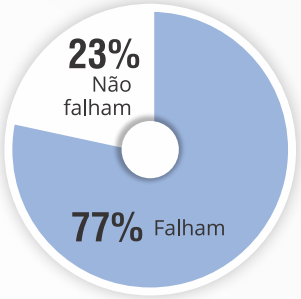
De acordo com pesquisa realizada pela Lieberman Software, a maioria dos profissionais da área de segurança de TI acredita que não.

Pesquisa com 200 participantes da RSA Conference 2016 (São Francisco, CA - EUA) apontou que, mesmo grandes corporações com segurança digital estabelecida, não estão preparadas para lidar com ataques cibernéticos.

A pesquisa teve como foco principal a utilização de senhas como método de verificação de identidade e a habilidade de soluções de segurança em prevenir ataques às organizações.

O principal motivo para insegurança é o nível de acesso que algumas senhas administrativas proporcionam e a dificuldade de mantê-las seguras.

FALHA NO USO DE SENHAS COMO MÉTODO DE SEGURANÇA



Principais causas:

1. Falta de atualizações frequentes nas identidades privilegiadas
2. Possibilidade de ex-funcionários acessarem os servidores após deixarem a organização
3. Facilidade com que as senhas são quebradas

Soluções:

1. Gerenciamento automatizado de identidades privilegiadas
2. Aplicação de valores únicos e complexos em cada uma das contas
3. Utilização de autenticação multi-fator.

DEFESA CONTRA ATAQUES CIBERNÉTICOS

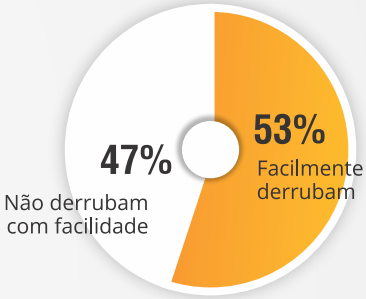
Principais causas:

1. Investimentos pesados não impediram vazamento e roubo de dados
2. Ferramentas convencionais de segurança como firewalls e sistemas de proteção/detecção de intrusão podem ser comprometidas por ferramentas avançadas.
3. Após invadir, basta comprometer uma identidade privilegiada e o intruso tem acesso à toda a rede

Soluções:

1. Atualização frequente de identidades privilegiadas, até mesmo em poucas horas
2. Credenciais com prazo limitado de validade e sem compartilhamento entre sistemas

HACKERS x SENHAS



Principais causas:

1. Modernas técnicas de ataques que facilitam a quebra senhas
2. Método de autenticação baseado em senhas de tamanho inadequado, baixa complexidade e baixa frequência de trocas – fatores fundamentais para o sucesso dos ataques
3. Tudo que o intruso realmente precisa, é de tempo

Soluções:

1. Automação no gerenciamento de políticas de senhas - idade, comprimento, complexidade e frequência de trocas
2. Uso da autenticação multi-fator
3. Diminuição na janela de tempo para que ataques sejam bem sucedidos

Em resumo, o maior problema de segurança enfrentado pelas organizações é garantir um bom gerenciamento das identidades privilegiadas, e um sistema automatizado que garanta a implementação de autenticação baseada em múltiplos fatores e prazo de validade limitado.

FONTE: RSA Conference 2016 Cyber Security Survey

Saiba mais sobre como o Gerenciamento de Identidades Privilegiadas pode proteger sua rede e responder de forma proativa a ataques cibernéticos. Entre em contato com a nossa equipe **comercial@hepta.com.br**

hepta

PARCEIRA OFICIAL:

LIEBERMAN SOFTWARE