**Boas praticas**

Com o avanço da tecnologia, nossas redes se tornam mais complexas e crescem mais a cada dia, e os hackers se tornam mais sofisticados. À medida que a discussão continua em torno de se novas vulnerabilidades devem ser divulgadas e se é bom oferecer cursos como escrita de vírus e invasão, precisamos proteger nossas redes. O desenvolvimento de uma estratégia de segurança sólida envolve balancear as mudanças nas ameaças e na tecnologia com nosso ambiente corporativo. Nem sempre é fácil saber como e o que proteger, e quais controles colocar em vigor. É preciso planejamento, procedimentos e desenvolvimento de políticas. O planejamento e a implementação para segurança da rede podem tomar muito tempo e sobrecarregá-lo. É aí que entram as melhores práticas. As melhores práticas são, na realidade, um conjunto de bons controles. Ao montar seu plano, certifique-se de que suas práticas incluem avaliação de riscos, prevenção, detecção, resposta e vigilância.

Aqui estão algumas das melhores práticas para ser capaz de detectar ataques pela rede:

* Considere diariamente que uma nova vulnerabilidade apareceu da noite para o dia.
* Faça parte da sua rotina diária verificar os arquivos de log em firewalls e servidores.
* Tenha uma lista de todos os produtos de segurança que você utiliza e verifique as atualizações nos
* Websites do fornecedor.
* Conheça sua infraestrutura de modo que possa detectar um comportamento anormal.
* Faça perguntas e procure respostas.

A seguir está um exemplo das melhores práticas para políticas de senha:

* Crie senhas com pelo menos oito caracteres, e exija o uso de letras maiúsculas e minúsculas, números e caracteres especiais.
* Bloqueie as contas do usuário após três a cinco tentativas de logon com falha. Isso evita programas que tentam decifrar senhas em contas bloqueadas.
* Monitore a rede em busca do uso de ferramentas questionáveis. Se os arquivos de senha puderem ser capturados, eles podem ser usados por programas de descoberta de senha em outra máquina.

Aqui está um exemplo de proteção da rede contra código malicioso:

* Instale software antivírus e atualize os arquivos regularmente. O software antivírus não causa bem algum à empresa se não for atualizado com frequência.
* Como você pode ver, colocar em funcionamento as melhores práticas tornará o ambiente de computação um local muito mais seguro. É preciso planejamento, teste e treinamento. Embora cada empresa deva ter seu próprio plano de segurança exclusivo, as melhores práticas podem ser compartilhadas entre as empresas.

A seguir estão alguns websites que oferecem boas informações sobre as melhores praticas

http://csrc.nist.gov/fasp/

http://www.cert.org/security-improvement/

http://www.sans.org/rr/

http://www.securityfocus.com