

Controlos mínimos na máquina da mãe, do pai, do cão e do periquito

Confraria Security & IT

Outubro 2009

Miguel Almeida

Agenda

- ❑ Quem é o gajo da gravata?
- ❑ Qual é o objectivo desta conversa?
- ❑ Essas máquinas valem alguma coisa?
- ❑ Reduzir riscos? Mas quais riscos?
- ❑ Os controlos base já não chegam?
- ❑ E quais é que tu propões?
- ❑ Hmm... como é que concretizamos isso?
- ❑ Ah, e tal... pois. E agora quem faz?
- ❑ Passa lá o comando ao próximo, vá...

Miguel Almeida

- ❑ Um artista lá do Sado, que já deu ~~20~~ 37 voltas ao Sol.
- ❑ Estudou no Técnico. Computadores ou lá o que era...
- ❑ Depois o pai ganhou juízo e mandou-o trabalhar.
- ❑ Começou a Safira. Trabalhou na Portucel e na Alitude.
- ❑ Depois cansou-se e foi p'ra Consultor.
- ❑ 7 anos na KPMG - *Manager* dos serviços de segurança.
- ❑ No final de 2007, mudou para a Deloitte. *Senior Manager* desses mesmos serviços. Foi uma passagem breve.

- ❑ Desde Janeiro de 2008, abraçou a carreira muito promissora de Consultor Independente, na área da sua especialização, ou seja, os Serviços de Segurança da Informação.

- ❑ Exemplos de clientes, aquelas casas que vestem o **rouge cerise** e o **azul profundo**.

Agora a sério: os objectivos *deste lero*

- ✦ Promover um projecto próprio da Confraria que vise publicar um documento e uma *tool* para:
 - ✦ Sensibilizar. Ajudar a compreender que os PCs lá de casa expõem as pessoas a riscos importantes;
 - ✦ Propor controlos viáveis. Identificar um conjunto mínimo de controlos, que sejam razoáveis, e que permitam limitar o risco a um patamar aceitável; e
 - ✦ Ajudar a configurar os controlos. Criar uma ferramenta que, de forma automática, defina a configuração preconizada pela Confraria.
- ✦ Lançar o mote. Chegar à frente. Dar o *kickoff*.

“Este PC não vale nada, ‘portantes’...”

Risco. Quando falamos em risco, falamos implicitamente em valor. Mas neste caso, qual é o valor?

- ❑ Os PCs contêm:
 - ❑ Fotografias, vídeos, músicas, documentos, mensagens, contactos, credenciais, etc.
 - ❑ Coisas pessoais e profissionais da mãe, do pai... *U got it :)*
- ❑ Já que pagámos o PC, esperamos que:
 - ❑ O desempenho seja adequado e previsível ao longo do tempo;
 - ❑ O sistema e os programas que vêm com a máquina sejam sempre confiáveis; íntegros. “Se lá está no ecrã, é porque é.”
- ❑ E já agora, se ‘tamos a pagar por Mbit à Internet, esperamos ter essa banda para nós.

“Ah!... sempre vale qualquer coisa”

Existe valor:

- ✦ Nos ficheiros em disco;
- ✦ No *speed* da máquina;
- ✦ Na integridade do sistema;
- ✦ Na banda disponível.

Riscos? Mas há alguma ameaça? (1)

Aos ficheiros?

Acesso ilegítimo e manipulação por:

- ✦ Acesso directo - proximidade física, local;
- ✦ Roubo do computador;
- ✦ Manutenção externa;
- ✦ Partilha mal controlada (via Internet); ou
- ✦ Vulnerabilidade num programa ou serviço.

E ainda... existe a ameaça de acesso a contas na Internet, no caso particular do acesso a *cookies* permanentes.

Riscos? Mas há alguma ameaça? (2)

Ao desempenho e à largura de banda?

Consumo de CPU, memória e banda excessivos por:

- ✦ Instalação / execução arbitrária de binários que consomem recursos em *background*;
- ✦ Múltiplas estirpes de *malware*; ou
- ✦ Configuração inadequada do sistema ou programas que afectam todos os utilizadores.

Riscos? Mas há alguma ameaça? (3)

À integridade do sistema e aplicações?

Alteração e adição de componentes essenciais por:

- ❖ Instalação de **loggers* e *trojans*; ou
- ❖ Múltiplas estirpes de *malware*.

A integridade dos componentes é fundamental para garantir, entre outros aspectos, (i) a protecção dos ficheiros, (ii) a confidencialidade dos dados, credenciais e comunicações, e (iii) a auditabilidade das operações, se for necessária.

E essas coisas são prováveis?...

- ✧ A probabilidade de ser alvo de algum (ou de vários) destes ataques tende para 1;
- ✧ O sucesso do ataque depende de dois factores:
 - ✧ Dos controlos técnicos de segurança activos; e
 - ✧ Da sensibilidade e inteligência dos alvos.*
- ✧ Esta conversa, esta proposta, visa o primeiro factor; o segundo fica para outra ocasião.

* Se um gajo for mesmo-mesmo parvo e correr toda a porcaria que lhe oferecem, a probabilidade já não tende para 1; *É 1*. E é quase merecido. "Quase?"... hmmm...

“So what?” The impact, I hear u ask?

O menu. Potencial, bem entendido.

- ❑ Exposição da vida privada;
- ❑ Informação profissional comprometida;
- ❑ Informação destruída ou inacessível;
- ❑ Contas bancárias vazias;
- ❑ Identidade comprometida;
- ❑ Participação em ataques a outros sistemas;
- ❑ Envio de publicidade ao Viagra e outras curas para o reumático;
- ❑ Máquinas e acesso à Internet lentas-comó-caracol :)
- ❑ (e mais coisas que agora não lembro porque já é tarde...)

Nada disto tem importância? Sim, sim... conta-me histórias...

Zen

O problema, em resumo:

- ❑ Há valores importantes;
- ❑ Há ameaças concretas;
- ❑ Os ataques são prováveis; e
- ❑ O impacto pode ser elevado.

E até há um bonequinho neste slide a
abrilhantar o PowerPoint*.

* disseram-me que 'tá na moda, e não sei quê... (?)



+ a sério: o que temos não chega? (1)

- ❑ Pelo sucesso dos ataques que podemos observar, e.g. *worms*, *vírus*, *botnets*, informação exposta, etc., não, não chega;
- ❑ Os controlos de segurança nas máquinas estão melhores mas, em muitos dos casos, não estão activos, e.g. contas sem privilégios, requisitos de complexidade nas *passwords*, cifra dos discos, etc;
- ❑ Até há pouco tempo, os controlos activos após instalação, no Windows e MacOS X (as múltiplas encarnações de Linux davam para outra conversa), incluíam, no melhor cenário:
 - ❑ *Firewall* (que pode ser facilmente desligada e/ou ter excepções);
 - ❑ Actualizações automáticas (do sistema operativo e algumas apps);
 - ❑ Anti-spyware (Windows Defender - básico)
- ❑ E existem vários serviços de rede activos que, na verdade, nem são necessários na máquinas lá de casa, e.g. Partilha de ficheiros.

+ a sério: o que temos não chega? (2)

Mas uma parte significativa dos ataques são bem sucedidos porque existe participação activa, embora inadvertida, dos utilizadores, não é? Como é que os controlos técnicos vão ultrapassar ISSO?

Boa pergunta; algumas respostas:

- ✦ Reduzindo o leque de opções actual, procurando manter a funcionalidade mais importante;
- ✦ Segregando as funções de administração e utilização;
- ✦ Protegendo o conteúdo das máquinas; e
- ✦ Limitando a superfície de exposição do sistema.

É um objectivo distinguir os contextos de administração e utilização.
Ok, porreiro. Conversa de consultor... E isso traduz-se em quê?

'A' proposta v0.1 (1)

❑ Preparar um documento que inclua, no mínimo:

- ❑ Um *statement* sobre a necessidade de reforçar os controlos;
- ❑ Um capítulo de sensibilização para os riscos;
- ❑ Um capítulo com a descrição dos controlos activados;
- ❑ Um capítulo sobre a utilização pós-*hardening*; e
- ❑ Um capítulo mais avançado para *die-hards* que queiram reverter algum parâmetro.

❑ Criar uma ferramenta que faça uma configuração:

- ❑ Por *Group Policy Objects* (GPOs);
- ❑ Por *Access Control Lists* (ACLs) nos ficheiros e chaves do *Registry*;
- ❑ Pela introdução de chaves no *Registry*;
- ❑ Pela modificação de alguns ficheiros; e/ou
- ❑ Pela execução de comandos para acções específicas.

E quais são os controlos a reforçar? *Next slide...*

'A' proposta v0.1 (2)

- ❑ Criar contas para utilizadores standard;
- ❑ Reforçar os requisitos de complexidade das *passwords*;
- ❑ Remover permissões de escrita arbitrária nos discos - limitar à *homedir*;
- ❑ Activar criptografia nos discos;
- ❑ Remover privilégios de execução de programas não-instalados a todos os utilizadores standard, incluindo binários, ActiveX e macros;
- ❑ Remover privilégios de instalação de ActiveX a todos os utilizadores standard;
- ❑ Inibir a desactivação da *firewall* e introdução de excepções;
- ❑ Inibir a desactivação das actualizações automáticas;
- ❑ Activar *screensaver* automático;
- ❑ Desactivar *autoplay* em todos os dispositivos;
- ❑ Desactivar serviços desnecessários;
- ❑ Retirar o *bind* de serviços desnecessários, nas interfaces;
- ❑ Activar o mecanismo *antiphishing* (discutível...);
- ❑ Activar *backup* automático ou, se não for exequível, activar um alerta periódico;
- ❑ Tornar o *desktop* administrativo, *very unpleasant* :)
- ❑ ...

Uns *bitaites* para o Plano de Projecto

- ❑ Identificar os controlos que podem ser reforçados, sem perda significativa de funcionalidade, partindo das GPOs, ACLs e privilégios instalados por omissão;
- ❑ Identificar a forma, a técnica, que permite activá-los através de um processo automatizado;
- ❑ Criar o automatismo para todos os controlos;
- ❑ Testar exaustivamente;
- ❑ Preparar o doc de contexto e manual;
- ❑ Publicar e publicitar junto dos media, OEMs, etc.
- ❑ Manter.

Quem faz? O papel da Confraria

Porquê a Confraria?

- ❑ Porque reúne uma colecção de *geeks* com conhecimento sobre o tema;
- ❑ Porque não é uma organização formal e tem mantido a neutralidade adequada;
- ❑ Porque não tem uma agenda secreta nem as colunas de débito e de crédito...

Quem faz? São precisos voluntários para:

- ❑ Seleccionar os controlos e as configurações;
- ❑ Programar a *tool*;
- ❑ Escrever o doc;
- ❑ Testar e rever os resultados;
- ❑ Sincronizar e gerir a bicharada;
- ❑ Publicar e publicitar; e
- ❑ Manter e dar apoio aos utilizadores.

RU On? :)

Quase-quase no fim...

Q&A

Contactos



Miguel Almeida

Consultor Independente

Serviços de Segurança da Informação

- ✘ +351 962 608 928
- ✘ miguelalmeida@miguelalmeida.pt
- ✘ www.miguelalmeida.pt

- ✘ linkedin.com/in/mjnalmeida
- ✘ facebook.com/mjnalmeida
- ✘ twitter.com/mjnalmeida



FIHANKRA. "casa/edifício" - símbolo de segurança. Os símbolos *Adinkra* foram criados originalmente pela tribo *Akan* do Gana e pela tribo *Gyaman* da Costa do Marfim, na África Ocidental. Os símbolos representam conceitos ou aforismos. São utilizados em tecidos, murais, cerâmica, marcenaria, e logos. São muitas vezes utilizados para transmitir mensagens que evocam facetas da vida das pessoas.