

Apresentação

Boa tarde eu chamo-me Ricardo Silva, sou gestor do site rsoutlook.com (site em português exclusivamente dedicado ao Outlook), sou autor dos livros Domine a 110% o Outlook 2003/XP e 2000 (livros para utilizadores avançados) e sou há 3 anos consecutivos MVP - nomeado pela Microsoft devido ao meu contributo nos Newsgroups portugueses. Gostaria de salientar que todos os assuntos que abordar nesta apresentação estão explicados detalhadamente no meu site ou nos meus livros.

Introdução à Segurança no MS-Outlook

O Outlook é um programa de correio electrónico poderoso e bastante flexível. Um dos grandes atractivos é a possibilidade de programação com o Visual Basic for Applications (VBA), que permite a todo o tipo de programadores criar um vasto leque de add-ins e ferramentas para melhorar o Outlook.

No entanto – e infelizmente – como todas as grandes ferramentas (como serras eléctricas, espingardas de caça, dinamite, ...) este poder pode ser mal utilizado por “criminosos” para espalhar vírus através de scripts que o próprio Outlook permite correr.

Para além disto, estes criminosos encontraram outras manhas para fazer com que o seus códigos malignos entrem na sua caixa de correio.

Felizmente a equipa que desenvolve o Outlook aprendeu com alguns destes truques e no Outlook XP incluíram um conjunto de ferramentas de segurança, que protegem os computadores e redes destes ataques.

Estas ferramentas estão espalhadas por diversas categorias; as mais interessantes estão ligadas á protecção contra vírus e outros tipos de código maléfico e algumas opções de protecção das mensagens como as assinaturas digitais e a encriptação.

Durante esta apresentação vou abordar alguns aspectos relacionados com a segurança no Outlook, são eles:

- Segurança de ficheiros anexos
- Opções de segurança do Outlook
- Restrição de acções dos programas externos
- Bloqueio de conteúdo externo
- Spam
- Hoaxes / Phishing
- Users Awareness – Prevenção para os utilizadores
- Outras questões relacionadas com segurança
- E se sobrar algum tempo irei ainda abordar:
 - Assinaturas digitais
 - Gestão de direitos / Rights management

Segurança de Ficheiros anexos

Uma das ferramentas mais faladas do Outlook é a sua capacidade de “remover” alguns tipos de anexos.

Esta ferramenta é útil uma vez que os utilizadores tendem a abrir os ficheiros anexos mesmo quando provêm de remetentes desconhecidos, levando ao contágio do seu computador (e de outros) com vírus e cavalos de troia.

Seja um utilizador doméstico ou um administrador de rede a primeira medida preventiva que deve tomar é instalar um bom programa de anti-virus em todos os computadores pelos quais é responsável e mantê-lo actualizado.

Os administradores podem controlar que tipos de ficheiros anexos podem estar ou não disponíveis para os utilizadores:

Os tipos de ficheiro do nível 1 (exe, bat, vbs, etc), são bloqueados pelo Outlook, não sendo possível ao utilizador aceder ao anexo.

Se for do nível 2 e tentar abrir o ficheiro vai aparecer uma mensagem para guardar o anexo no disco. Esta opção é especialmente útil se o utilizador possuir um antivírus activo e devidamente actualizado porque ao guardar o anexo, o vírus será detectado podendo deste modo o antivírus actuar com segurança.

Se for do nível 0 vai poder abrir este ficheiro directamente do Outlook. O que significa que não existem restrições.

Proteger o Outlook contra HTML, Controlos e Scripts malignos

O Outlook pode enviar e receber mensagens HTML. Uma vez que estas mensagens podem conter scripts que são executados quando uma página é visualizada, alguns “hackers” utilizaram esta opção para atacar o comum utilizador.

Para prevenir qualquer dano com este tipo de código o Outlook desactiva automaticamente scripts e controlos ActiveX nas mensagens recebidas.

Pode ainda ter maior controlo configurando as zonas de segurança – baseadas na mesma filosofia do Internet Explorer.

Restringir as acções de programas externos

O Outlook sempre permitiu que programas externos (programas de sincronização como ActiveSync, PalmOS e a ferramenta de Mail-Merge do WinWord) acessem ao livro de endereços para criar ou ler mensagens.

O Outlook XP restringe a actividade de alguns programas externos prevenindo as consultas aos livros de endereços, envios de mensagens em nome doutrem, ou guardar ficheiros “perigosos” no disco. Para ser mais preciso, o Outlook passará a avisar sempre que um programa externo tenta fazer alguma destas acções; no entanto os programadores podem trabalhar com o Outlook para que este reconheça as suas aplicações como legítimas. Se se utilizar um Exchange Server, pode definir exactamente que opções queremos ou não permitir.

Bloqueio de conteúdo externo

Na versão mais recente do Outlook (a 2003) e se o padrão de instalação não for alterado o programa impede a transferência automática de alguns conteúdos externos (ex: imagens) desta forma ajuda a proteger a privacidade de cada utilizador.

As imagens de correio electrónico em HTML podem fazer com que o Outlook as transfira de um servidor. Ao comunicar com um servidor externo é possível verificar a validade do endereço de correio electrónico para o remetente, tornando-o possivelmente no alvo de mais mensagens de publicidade não solicitada (spam)

Spam

Em Portugal, uma grande percentagem de utilizadores do correio electrónico recebe mensagens indesejadas, mensagens com conteúdo não solicitado e por conseguinte considerado lixo electrónico.

O Spam (termo que não tem tradução significando apenas correio electrónico não solicitado) é considerado um dos maiores problemas dos utilizadores da Internet. São na sua maioria mensagens publicitárias, tentativas de burla, mensagens com conteúdo sexual e muitas vezes de produtos duvidosos ou esquemas de lucro fácil, propostos a uma grande lista de utilizadores.

Existe um grande negócio em volta das mensagens de correio electrónico, existem diversas entidades a vender bases de dados com milhares ou até milhões de endereços de correio electrónico. (- Num artigo recente sobre a prisão de um spammer americano li que este

individuo tinha 16 linhas dedicadas de alta velocidade em sua casa, enviando diariamente cerca de 10 milhões de mensagens, produzindo uma receita na ordem dos 750 mil dólares/mensais.)

Seguem-se alguns Conselhos Úteis no Combate ao Spam

Neste momento existem algumas alternativas para combater o spam a primeira será adquirir software específico para combater este problema, mas parece-me que a solução mais adequada seja a prevenção. Pode gastar muito dinheiro e mesmo assim ninguém lhe fornecerá a garantia a 100% que se vai livrar deste problema de uma vez por todas.

No entanto, existem métodos que podem reduzir substancialmente a quantidade de lixo que recebe na sua caixa de correio. São eles:

- Utilizar os filtros do Outlook 2003 para gerir os remetentes de spam;
- Não responder a mensagens de spam;
- Ao colocar questões em newsgroups dar um endereço de correio electrónico falso;
- Nunca dar o seu endereço de correio electrónico primário;
- Utilizar a lei contra o spam;
- Não colocar o seu endereço no seu site ou protegê-lo com script;
- Ler as políticas de privacidade de alguns sites;
- Não reencaminhar mensagens em cadeia.

Hoaxes / Phishing

Os hoaxes não são nem virus, nem worms, nem cavalos de troia, são partidas enganosas para os utilizadores. Alguns pretendem que os utilizadores acreditem que vão ser atacados por um vírus extremamente perigoso (e dão indicações erradas de como se proteger), mais recentemente associados a este fenómeno são mensagens que pedem aos utilizadores para confirmarem ou fornecerem dados pessoais alegando algum pedido de crédito ou de acesso a site financeiro – este fenómeno mais recente também é conhecido por Phishing.

É conveniente explicar aos utilizadores como identificar este tipo de mensagens e também explicar-lhes como evitá-las.

User Awareness

Os utilizadores são a “arma” mais perigosa contra uma rede – li num artigo que 60% dos ataques a redes provêm de fontes internas. São os utilizadores as “firewall” das nossas redes, porque são eles que em última instância tem o poder de executar um ficheiro anexo que pode conter vírus e infectar toda a rede.

É muito importante avisar os utilizadores dos perigos que podem causar quando abrem determinados tipos de ficheiros.

É ainda mais importante explicar aos utilizadores que não devem abrir mensagens de desconhecidos, não fornecer qualquer tipo de informação sensível por e-mail e ensiná-los a combater o correio electrónico não solicitado (spam).

As actualizações dos produtos Windows/Office desempenham um papel fundamental para os utilizadores se manterem “seguros” contra possíveis falhas ou lacunas dos softwares.

Outras questões relacionadas com segurança

Perguntam-me com alguma frequência se o painel de pré-visualização é seguro ?

Na minha opinião é, e passo a explicar:

A ferramenta de bloqueio de anexos e o patch de segurança para o Iframe do Internet Explorer que foram lançados pela Microsoft em 2000 e 2001 respectivamente dão ao painel de pré-visualização uma maior segurança.

Cada versão do Outlook é mais segura que a anterior, dando aos administradores poucas razões para desabilitar o preview pane. Como sempre, a melhor solução é bloquear mensagens nos servidores ou gateways, o que significa que poucos ou nenhum virus chegará às caixas de correio. Um administrador responsável removerá ficheiros executáveis no lado do servidor.

Desactivar o Out of Office para o exterior, Desactivar recibos automáticos e Reverificar os endereços antes de enviar.

Estes 3 assuntos estão relacionados, o objectivo é evitar a saída de informação desnecessária ou por engano. No caso do Out of Office e dos recibos automáticos evitam-se as confirmações de endereços de correio electrónico para possíveis Spammers.

Proteger mensagens com encriptação e assinaturas digitais

O Outlook suporta o Secure Multipurpose Internet Mail Extensions, ou S/MIME desde a versão 2000. S/MIME é um conjunto de protocolos de segurança que permite que as mensagens sejam protegidas contra **tampering** e **eavesdropping**. As mensagens enviadas entre 2 programas compatíveis com S/MIME podem ser assinadas digitalmente, encriptadas ou assinadas e encriptadas.

A protecção das mensagens de correio electrónico oferece algumas vantagens aos utilizadores. Em primeiro lugar – a autenticação – ou seja, o destinatário pode provar que na realidade a mensagem é do remetente, uma vez que esta vem assinada através do certificado digital. Em segundo lugar – a privacidade – já que é assegurado que apenas o destinatário pode ler a mensagem, sendo esta imperceptível para as outras pessoas, através da encriptação.

Gestão de direitos

A gestão de direitos gere a transferência de informação confidencial ou sensível entre indivíduos. Se enviar uma mensagem a informá-lo da má conduta de um colega seu, a última coisa que pretende é que o seu chefe reenvie essa mensagem para esse colega. Nesta ordem de ideias também não vai querer que o seu chefe imprima uma cópia dessa mensagem. A gestão de direitos dá ao autor controlo sobre o conteúdo criado. No Outlook os autores podem utilizar a gestão de direitos para impedir que uma mensagem seja reenviada, impressa, copiada ou distribuída sobre outra forma.

A gestão de direitos pode funcionar a dois níveis – empresarial e pessoal.

No nível empresarial existe um servidor onde é instalada a aplicação de gestão de direitos e onde estão configuradas as permissões para cada utilizador. Assim é necessário que tanto o remetente como o destinatário tenham contas nesse servidor.

No nível pessoal (ou para uso na empresa se não quiser investir num servidor) pode utilizar o Microsoft Passport para se autenticar nos servidores públicos da Microsoft. O funcionamento é idêntico ao exposto anteriormente, com a excepção de que terá que estar ligado à Internet para se autenticar e que terá que criar uma conta Passport para poder utilizar esta ferramenta.

Conclusão

Dando por concluída esta apresentação gostaria de realçar que a mesma se encontrará disponível para download no meu site.

“O Outlook é mais do que um programa de correio electrónico é uma ferramenta de segurança”