

www.rsoutlook.com

Segurança no MS-Outlook


Vantagem+ Security 2004 - Security, Disaster Recovery e Storage Management

Ricardo Silva
Rsoutlook.com
Vantagem+ Security 2004
Lisboa
24 de Novembro de 2004

Temas a abordar

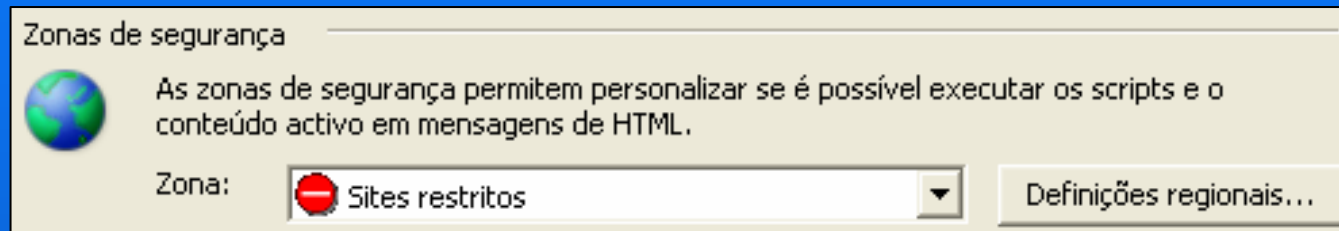
- ◆ Segurança de ficheiros anexos
- ◆ Opções de segurança do Outlook
- ◆ Restrição de acções dos programas externos
- ◆ Bloqueio de conteúdo externo
- ◆ Spam
- ◆ Hoaxes / Phishing
- ◆ Users Awareness
- ◆ Outras questões relacionadas com segurança
- ◆ Talvez aborde estes se houver tempo:
 - Assinaturas digitais
 - Gestão de direitos / Rights management

Segurança de Ficheiros anexos

 O Outlook bloqueou o acesso aos seguintes anexos potencialmente inseguros: ANIMAT10.EXE.

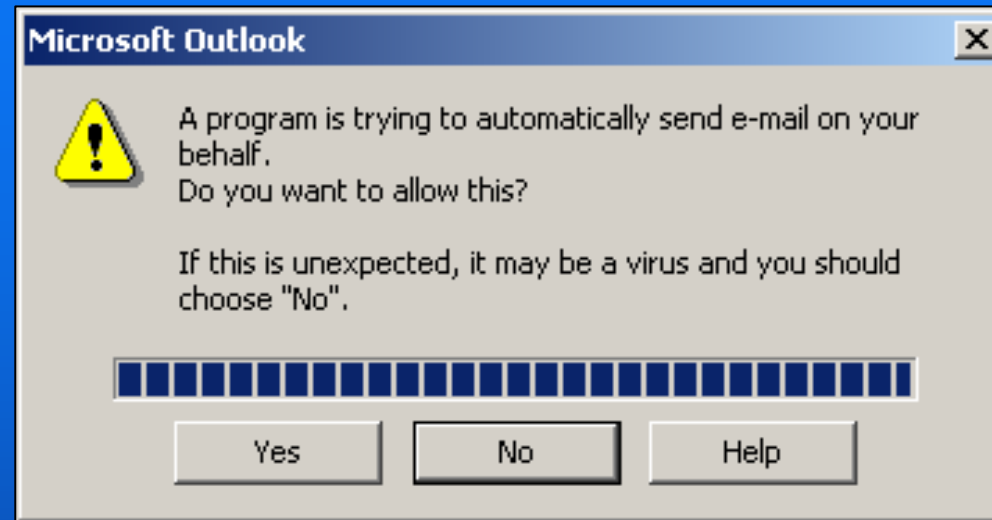
- ◆ **Opção com maior impacto para os utilizadores**
- ◆ **Bloqueio de ficheiros pelo seu grau de risco**
 - Nível 1
 - Nível 2
 - Nível 0
- ◆ **Solução Registry / Solução Administrativa**
- ◆ **Muitos utilizadores sabem como desbloquear (registry / third party)**

Opções de segurança no Outlook



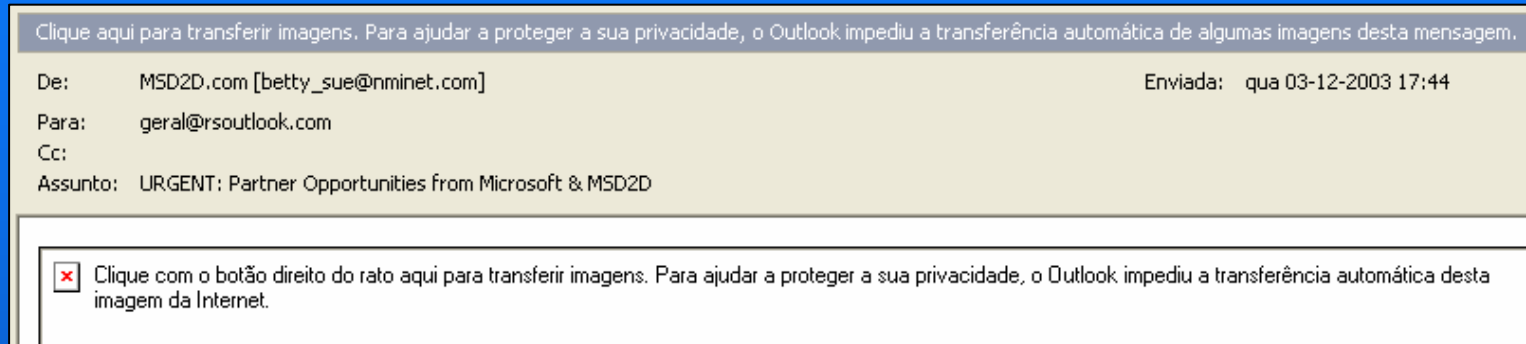
- ◆ Mensagens em formato HTML com *scripts* ou *ActiveX* não são executados, independentemente da zona de segurança que tenha definido.
- ◆ É de salientar ainda que a zona de segurança do *Microsoft Outlook* está definida para Sites restritos (*Restricted sites*) desde a instalação.

Restrição de acções dos programas externos



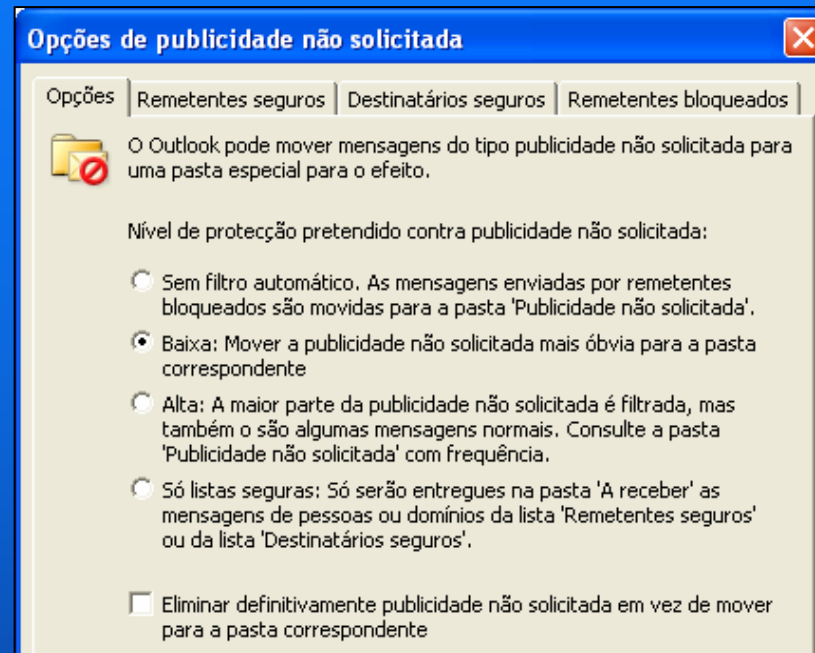
- ◆ O Outlook sempre permitiu que programas externos (ActiveSync, PalmOS e MailMerge do Word,...) acessem ao livro de endereços e criar ou enviar mensagens.
- ◆ Evitar o contágio dos nossos recursos.
- ◆ Dificultando a tarefa dos programadores.

Bloqueio de conteúdo externo



- ◆ Bloqueio de conteúdo externo (Internet) nas mensagens de tipo HTML.

Spam



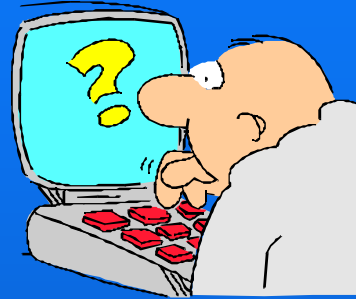
- ◆ Uma das principais novidades mais eficazes é o **Filtro publicidade não solicitada** (*Junk e-mail filter*).
- ◆ Este filtro ajuda a impedir a recepção diária de mensagens de correio electrónico indesejadas.

Hoaxes / Phishing



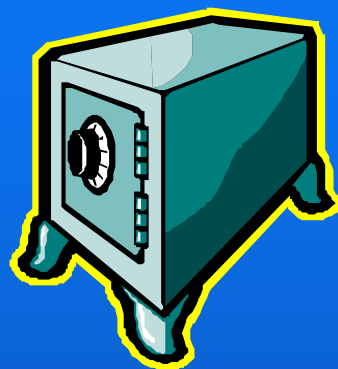
- ◆ Partidas - Não são nem vírus, nem worms, nem cavalos de Tróia, são partidas enganosas para os utilizadores. Pretendem que os utilizadores acreditem que vão ser atacados por um vírus extremamente perigoso.
- ◆ Explicar aos utilizadores como identificar este tipo de mensagens.
- ◆ Não seguir links para fornecer credenciais (phishing)

User Awareness



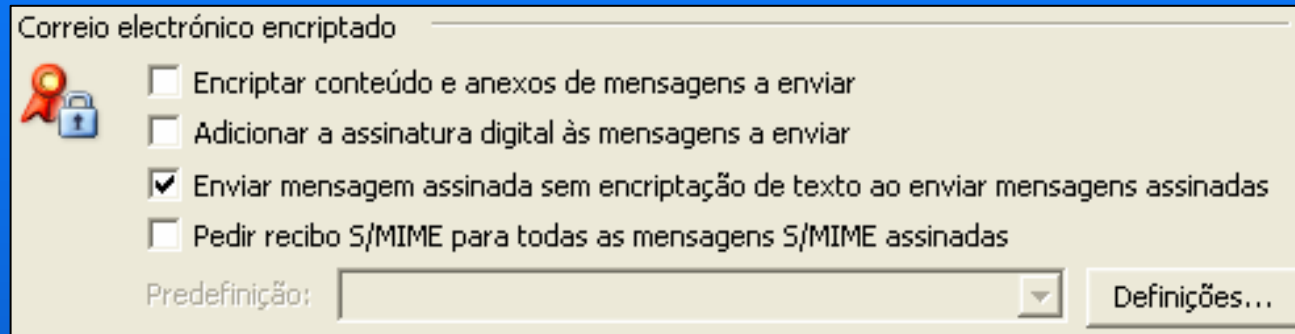
- ◆ Os utilizadores são as “firewalls” das nossas redes
- ◆ É muito importante explicar aos utilizadores que não devem abrir anexos perigosos.
- ◆ É mais importante explicar aos utilizadores que não devem abrir mensagens de desconhecidos.
- ◆ Não fornecer qualquer informação sensível por email
- ◆ Combater correio electrónico não solicitado (spam)
- ◆ Actualizações do produto Windows/Office

Outras questões relacionadas com segurança



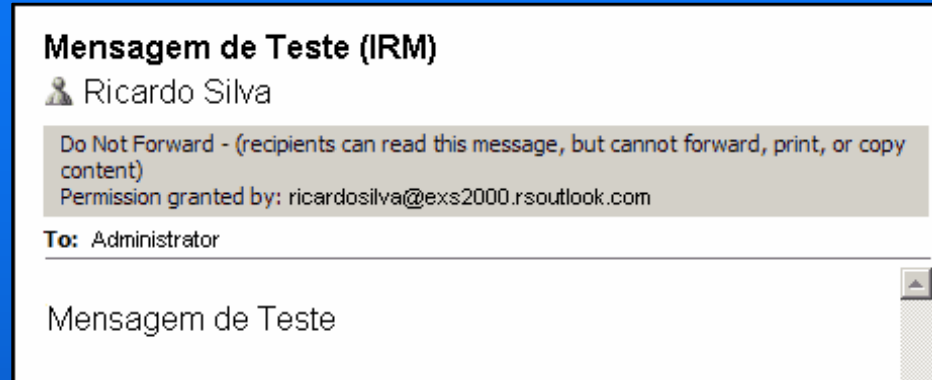
- ◆ Painel de pré-visualização (PreviewPane) – é seguro?
- ◆ Out Of Office – Desactivar para o exterior.
- ◆ Desactivar recibos automáticos para o exterior.
- ◆ Re-verificar os endereços antes de enviar (para evitar saídas de informação por engano) .

Assinaturas digitais



- ◆ O Outlook suporta o Secure Multipurpose Internet Mail Extensions,
- ◆ S/MIME é um conjunto de protocolos de segurança que permite que as mensagens sejam protegidas contra *tampering* e *eavesdropping*.

Gestão de direitos / Rights management



- ◆ O serviço de **Gestão de direitos (*Rights management*)** para mensagens de correio electrónico e para documentos de *Office* em anexo. A **Gestão de direitos** é uma tecnologia destinada a ajudar a proteger as informações digitais contra utilizações não autorizadas.

www.rsoutlook.com

Segurança no MS-Outlook

Contactos

Ricardo Silva

ricardosilva@rsoutlook.com

www.rsoutlook.com

Ricardo Silva
Rsoutlook.com
Vantagem+ Security 2004
Lisboa
24 de Novembro de 2004