Serviços de Informática da Universidade Aberta

Manual de Boas Práticas

Temas:

- **Cuidados a ter com os anexos do correio eletrónico (*email*)**
- **Navegar na internet de forma segura: Conteúdo Ativo e as *Cookies***
- **Avaliação das Definições de Segurança do seu Navegador (*Browser*) *Web***
- **Atualizações de *Software* (*Patches*)**

Cuidados a ter com os anexos do correio eletrónico (*email*)

O *email* circula com facilidade, e o seu reenvio é tão simples que os vírus podem rapidamente infetar um grande número de máquinas. Alguns dos vírus até são capazes de detetar todos os endereços de email presentes na máquina do utilizador e enviar-lhes mensagens infetadas.
Praticamente qualquer tipo de ficheiro pode ser anexado a uma mensagem de email, pelo que os atacantes têm uma grande liberdade na escolha dos tipos de vírus que podem enviar.

Para nos protegermos a nós e á nossa lista de endereços devemos:

Desconfiar de quaisquer anexos que nos sejam enviados, mesmo de pessoas que conhecemos – Só porque um *email* parece ter vindo de um familiar, amigo ou colega, tal não quer dizer que isso tenha realmente acontecido. Muitos vírus conseguem alterar (diz-se que fazem "*spoof*") o endereço de origem, fazendo com que a mensagem pareça ter tido origem noutra pessoa. Se possível, verifique junto da pessoa que terá enviado a mensagem, para garantir que esta é legítima, antes de abrir quaisquer

anexos. Isto inclui mensagens que pareçam ter vindo do seu administrador de sistemas, ou do fabricante de *software*, as quais indicam que incluem atualizações (*patches*) ou software antivírus. Tanto os administradores de sistemas como os fabricantes de *software* não enviam atualizações através de mensagens de *email.*

Manter o *software* atualizado – Instale atualizações de ***software*** para que os atacantes não possam usar para seu proveito os problemas e vulnerabilidades conhecidos. Muitos sistemas operativos oferecem a capacidade de instalar estas atualizações automaticamente. Sempre que esta opção estiver disponível, deve ser aproveitada.

Confiar nos nossos instintos – Se um *email* ou os seus anexos parecem suspeitos, não os abra, mesmo que o *software* antivírus indique que a mensagem é segura. Os atacantes lançam constantemente novos vírus, e o seu *software* antivírus pode ainda não reconhecer esse vírus. No mínimo, contacte a pessoa que enviou a mensagem antes de abrir qualquer anexo. Não esqueça que mesmo as mensagens que parecem ter sido enviadas por pessoas em que confia podem conter vírus. Se houver alguma coisa na mensagem que lhe pareça estranho, pode haver uma razão para isso. Não deixe que a sua curiosidade coloque o computador em risco.

Guardar os anexos e fazer um *scan* com o antivírus antes de os abrir – Se tiver que abrir um anexo antes de poder verificar a sua origem, tome os seguintes passos:

- ✓ Assegure-se que o seu programa de antivírus está atualizado (execute uma atualização do antivírus se não tiver a certeza).
- ✓ Grave os anexos no computador ou num disco.
- ✓ Efetue um scan manual dos anexos, utilizando o programa de antivírus.
- ✓ Se o resultado final for que os anexos se encontram limpos, só então os deve abrir.

Considerar a criação de contas separadas no computador – Os utilizadores com privilégios de "administrador" podem considerar a opção de ler o seu *email* através de uma conta com privilégios restritos. Alguns vírus requerem privilégios de "administrador" para infetar um computador.

Navegar na *internet* de forma segura: Conteúdo Ativo e as *Cookies*

Para aumentar a funcionalidade ou adicionar características avançadas, os *sites web* muitas vezes socorrem-se de *scripts* (conjuntos de instruções) que executam programas dentro do *browser.*

Este conteúdo ativo pode ser usado para criar, por exemplo, "*splash pages*" (conteúdo que ocupa toda a página do *browser* momentaneamente) ou opções como a utilização de menus tipo "*dropdown*".

Infelizmente, estes *scripts* são uma forma de um atacante descarregar conteúdo malicioso para o computador do utilizador.

O *JavaScript* é apenas um de muitos tipos de *scripts* da *web* (existem outros como *VBScript, ECMAScript*, ou *JScript*), embora seja talvez o mais reconhecido. Utilizado em praticamente todos os *sites web*, o *JavaScript* e outros tipos de *scripts* são populares porque os utilizadores nesta altura já esperam a aparência e funcionalidade que este permite, sendo muito fácil de incorporar nas páginas (uma grande parte das aplicações de desenvolvimento de conteúdos para a *web*, têm a capacidade de adicionar elementos em *JavaScript* sem necessidade de grandes conhecimentos por parte do programador). No entanto, e por estas mesmas razões, os atacantes podem manipulá-lo para os seus próprios fins. Um tipo de ataque muito popular, que se baseia em *JavaScript*, envolve o redireccionamento dos utilizadores de um *site* legítimo, para outro malicioso, onde sejam descarregados vírus ou recolhida informação pessoal.

O *Java* e os controlos *ActiveX* são verdadeiros programas que residem no computador ou que podem ser descarregados pela rede até ao seu *browser.* Se executados por atacantes, estes controlos *ActiveX* são capazes de efetuar no computador tudo que o utilizador legítimo também é capaz (e podem executar programas maliciosos de *spyware* e recolher informação pessoal, ligarem-se a outros computadores e potencialmente provocar outros danos). Os programas *Java (Java applets*) são normalmente executados num ambiente mais restrito, mas se esse ambiente não for seguro, então os programas *Java* podem igualmente criar oportunidades para ataques.

O *JavaScript* e outros tipos de conteúdo ativo nem sempre são perigosos, mas são na verdade ferramentas comuns dos atacantes. É possível prevenir a execução de conteúdo ativo na maior parte dos *browsers*, mas essa segurança adicional pode limitar funcionalidades e eliminar características de alguns dos *sites* visitados. Antes de *clicar* num *link* para um *site web* que não conhecemos ou em que não confiamos, deve ser desabilitada a execução de conteúdo ativo.

Estes mesmos riscos também se podem aplicar ao programa de *email* que usamos. Muitos clientes de *email* usam os mesmos programas que são usados pelos *browsers* para mostrarem mensagens em HTML. Como tal, muitas das vulnerabilidades que afetam conteúdos ativos como *JavaScript* ou *ActiveX*, também se podem aplicar ao *email*.

A escolha de visualizar as mensagens de *email* como texto simples é uma forma de resolver estes problemas.

O que são *cookies*?

Quando se navega pela *Internet,* existe informação sobre o computador que pode ser recolhida e guardada (por exemplo, o endereço IP da máquina, o domínio utilizado para a ligação .pt, .com, .net, ou o tipo de *browser* utilizador). Pode também ser informação mais específica sobre o seu estilo de navegação (como a última vez que foi visitado determinado *site*, ou as suas preferências pessoais de visualização).

Os *cookies* podem ser guardados por diferentes períodos de tempo:
• ***Cookies* de sessão** (*Session cookies*) – O *cookies* de sessão guardam informação apenas enquanto se está a utilizar o *browser*. Uma vez que o *browser* seja fechado, a informação é apagada. O objetivo principal dos *cookies* de sessão é ajudar a navegação, por exemplo indicando se já visitámos determinada página e retendo informação sobre as suas preferências após ter visitado a página.
• ***Cookies* persistentes** (*Persistent cookies*) – Os *cookies* persistentes são guardados no computador de forma que as suas preferências pessoais possam ser retidas. Na maior parte dos *browsers*, é possível ajustar o período de tempo de guarda destes *cookies*. É devido a estes *cookies* que o seu endereço de *email* aparece quando se abrem as páginas dos *emails* do *Yahoo* ou do *Hotmail*. Se um atacante conseguir aceder ao seu computador, pode obter informação pessoal sobre si através destes ficheiros.
De forma a aumentar o seu nível de segurança, considere o ajuste dos seus níveis de segurança de forma a bloquear ou limitar as *cookies* presentes no *browser*. Para que outros *sites* não possam recolher informação pessoal sobre si, sem o seu consentimento, selecione a opção de só permitir os *cookies* para o *site web* que está nesse momento a ser visitado; bloqueie ou limite o acesso às *cookies* para quaisquer terceiras partes. Se estiver a utilizar um computador partilhado, deve garantir que as *cookies* estão desabilitadas, de forma a impedir que outras pessoas usem ou acedam à sua informação pessoal.

Avaliação das Definições de Segurança do seu Navegador *(Browser) Web*

O *browser web* é a sua ligação primária para toda a *Internet*, e muitas aplicações podem funcionar com base nele, ou em componentes dele.
Isto faz com que a escolha das definições de segurança do *browser web* sejam muito importantes.
Existem também muitas aplicações *web* que tentam melhorar a sua experiência de utilização através da alteração dos parâmetros de segurança. No entanto, estas alterações podem não ser necessárias e, no limite, podem mesmo deixá-lo suscetível de ser atacado. A regra de ouro é que a maioria das definições sejam desabilitadas, a menos que se decida que estas são necessárias.
Se conseguir determinar que um *site* específico é seguro, pode escolher habilitar estas definições temporariamente, e posteriormente, ao sair do *site*, voltar a desabilitá-las.

Embora cada *browser* tenha definições que estão selecionadas por omissão, pode vir a descobrir que o *browser* também contém níveis de segurança que são selecionáveis. Por exemplo, o *Internet Explorer* oferece definições

adaptadas por defeito ao nível de segurança escolhido; as características/opções estão habilitadas/desabilitadas de acordo com esse nível de segurança.
No entanto, e mesmo com estas facilidades, ajuda ter um entendimento do que cada um dos diferentes termos significa, de forma a poder conscientemente avaliar quais as definições mais apropriadas para o seu caso.

Idealmente, cada definição de segurança deveria ser selecionada para o mais alto nível de segurança possível. No entanto, a restrição de algumas características pode limitar o carregamento ou funcionamento de algumas páginas *web.*
A melhor opção será sempre a adoção do nível mais alto de segurança e a habilitação de algumas características apenas quando as suas funcionalidades sejam necessárias.

Diferentes *browsers* utilizam diferentes termos, mas aqui estão alguns termos e opções que poderá encontrar:
Zonas (*Zones*) – O seu *browser* pode dar-lhe a opção de colocar *sites web* em diferentes segmentos, ou zonas, definindo diferentes restrições de segurança para cada zona. Por exemplo, o *Internet Explorer* identifica as seguintes zonas:
Internet – Esta é a zona geral para todos os *sites web* públicos. Ao explorar a *Internet*, as definições desta zona são automaticamente aplicadas aos *sites* que visita. Para lhe dar a experiência mais segura de navegação, esta definição devia estar apontada para o mais alto/seguro. Se tal não for possível, deve mesmo assim ser mantido um nível, pelo menos, médio.
***Intranet* Local (*Local Intranet*)** – esta zona define a segurança das páginas internas e corresponde á nossa área privada. Dado que os conteúdos *web* estão normalmente disponíveis num servidor web interno, é normalmente seguro ter definições menos restritivas neste tipo de ambiente.
***Sites* Reconhecidos (*Trusted Sites*)** – Se acredita que alguns *sites* estão desenhados com muita segurança, e se considera que os conteúdos provenientes desses *sites* não contêm material malicioso, pode adicioná-los à lista de *sites* seguros e aplicar as definições de segurança de acordo com a sua escolha. Pode também obrigar a que só os *sites* que implementem *SSL (Secure Sockets Layer)* possam estar ativos nesta zona (o cadeado está indicado no *browser*, e as chamadas do *browser* implementam https://). No geral, este tipo de zona é opcional, mas pode ser útil se estiver a manter múltiplos *sites web* ou se a sua organização tem vários *sites.* No entanto, mesmo que sejam *sites* reconhecidos, evite sempre que possível aplicar definições de segurança de baixo nível – caso os sites sejam atacados, podemos por essa via ficar expostos.
Sites Restritos (*Restricted Sites*) – Se existem *sites* particulares que julgue não serem seguros, pode identificá-los e implementar definições de

segurança de nível acrescido. No entanto, e dado que as definições de segurança podem não ser suficientes, a melhor medida de precaução é evitar navegar em *sites* cuja segurança julgue ser duvidosa.

JavaScript – Alguns *sites web* utilizam instruções (*web scripts*), por exemplo em *JavaScript*, para conseguirem ter determinada aparência ou funcionalidades. Contudo estes *scripts* são vulneráveis a ataques. O *JavaScript* deve estar ativo apenas quando e se necessário.

Java* e controlos *ActiveX – Estes programas são usados para desenvolver ou executar conteúdo ativo que permite determinada funcionalidade. Tal como para o caso anterior, só deve estar ativo se necessário, dado o risco que representam.

Plug-ins – Por vezes os *browsers* requerem a instalação de *software* adicional, conhecido como *plug-in* e que permite a existência de determinada funcionalidade. Tal como os controlos *Java e ActiveX*, também os *plug-ins* podem ser usados num ataque. Como tal, antes de os instalar, garanta que necessita deles e que o site onde os obteve é de confiança.

Gestão de *cookies (Manage cookies)* – OS *cookies*, que mantém informação entre visitas a *sites*, podem ser habilitados, desabilitados ou restringidos. Na generalidade. A melhor escolha é desabilitá-los e apenas os reabilitar a quando da visita a um *site* que confiamos e que requer a sua presença.

Bloqueio de janelas de *pop-up (Block pop-up windows*) – Embora a habilitação desta funcionalidade possa restringir a utilização de alguns *sites web*, também irá minimizar o número de janelas de *pop-up* com anúncios que recebe, alguns dos quais podem ser maliciosos.

Atualizações de Software (Patches)

Os *patches* (em inglês, remendos), são utilizados para tapar ou reparar buracos nos programas. Os *patches* são atualizações que corrigem um problema em particular ou uma vulnerabilidade de um programa.

Quando os *patches* estão disponíveis, normalmente são colocados nos *sites* dos fabricantes para que os utilizadores os possam descarregar. É muito importante instalar um *patch* assim que possível, de forma a proteger o computador de ataques destinados a tirar vantagens dessa vulnerabilidade. Os atacantes podem tentar explorar a existência das vulnerabilidades durante meses ou anos após um *patch* corretivo ser lançado. Alguns tipos de *software* são capazes de verificar automaticamente a existência de novos *patches.* Se estas opções automáticas estiverem disponíveis, recomenda-se que tire partido delas.

Para os utilizadores com privilégios de "administrador" recomenda-se que apenas descarreguem *software* ou atualizações de *sites web* que conheçam. Não confiem em *links* recebidos por *email* – os atacantes usam mensagens de

email para direcionar os utilizadores para *sites* maliciosos, onde os utilizadores descarregam e instalam vírus, que chegam disfarçados de atualizações de *software*. Tenham especial cuidado com mensagens de *email* que indicam que o *patch* se encontra disponível como anexo – estes anexos são com frequência vírus.

28 de Abril de 2014