Proteção de Dados
https://www.uminho.pt/protecaodados
protecaodados@uminho.pt
Telefone: +351 253 510 006

Universidade do Minho

Título: Boas práticas - Medidas de segurança para sistemas informáticos provedores de serviços em linha (sistemas servidor)

1. Âmbito e Objeto

As boas práticas propostas neste documento são a orientação do Encarregado da Proteção de Dados para os responsáveis e administradores dos sistemas informáticos que disponibilizem serviços em linha[1] (sistemas servidor) em nome da Universidade do Minho (UMinho).
As medidas de segurança definidas visam estabelecer um padrão mínimo para a segurança dos referidos sistemas informáticos, devendo ser complementadas com medidas adicionais, adequadas à criticidade e sensibilidade da informação processada por esses sistemas. A criticidade e sensibilidade da informação deve ser considerada em relação aos interesses da UMinho e dos titulares dos dados quando se trate de dados pessoais.
As medidas para a segurança dos sistemas informáticos devem ser permanentemente geridas adaptando-se às alterações do contexto.
Este documento não aborda as necessárias medidas para a segurança física dos sistemas informáticos.

2. Princípio para a exposição de sistemas na Internet

Um sistema informático só deverá ser colocado diretamente exposto na Internet[2]. se disponibilizar serviços que devam estar acessíveis a pessoas sem conta nos serviços digitais da UMinho, ou serviços que não possam ser acedidos através de VPN.

3. Medidas de segurança essenciais para sistemas servidor

3.1. Incorporação, exploração e alienação de sistemas

- Todos os sistemas institucionais devem ser reinstalados de raiz antes de serem colocados ao serviço da UMinho.
- Todo o *software* instalado deve provir de fornecedores confiáveis e deve ser obtido de fontes oficiais.
- O *software* instalado deve ser apenas o necessário à função do sistema.
- Os sistemas servidor só devem permanecer acessíveis na rede enquanto estejam a ser ativamente utilizados, assim que se extinga o seu propósito devem ser retirados.
- Os sistemas servidor acessíveis na rede devem ter designado um administrador que garanta a sua gestão técnica, no mínimo a aplicação de atualizações de segurança e monitorização. Cabe ao responsável pelo sistema designar o seu administrador e providenciar a substituição na sua ausência.
- Todos os sistemas institucionais devem ser limpos de forma irreversível de quaisquer informações ou configurações quando terminem o seu serviço à UMinho.

3.2. Configuração segura, hardnening, zero trust

- Todas as *passwords* que tenham sido definidas pelo fabricante devem ser alteradas.
- Todas a contas criadas pelo fabricante que não venham a ser utilizadas devem ser desabilitadas.
- Os serviços desnecessários devem ser desabilitados.
- Os serviços oferecidos pelo sistema devem estar acessíveis do modo mais restrito possível, limitando, conforme se aplique, a endereços IP, portos, protocolos, etc., e quando possível, requerendo autenticação. (*zero trust: least privilege*)
- A restrição de acesso de acesso aos sistemas servidor, de acordo com a estrita necessidade, não deverá ter exceções, aplicando-se a todos os acessos, sejam eles internos ou externos. (*no trust by default*)

[1] 'Sistema informático que disponibilize serviços em linha' deve ser entendido de uma forma abrangente, como qualquer dispositivo que execute instruções que lhe sejam submetidas através da rede. Podem ser servidores web, servidores de ficheiros, impressoras, mas também dispositivos IoT como eletrodomésticos, fechaduras, termómetros, etc.
[2] Diretamente exposto na Internet deve ser entendido como tendo um endereço IP público. No endereçamento IP público atribuído à UMinho serão endereços IP começados por 193.136 ou 193.137.

- A tentativa de acesso por sistema autorizado, a funcionalidades diferentes daquelas a que está autorizado deve originar um alarme aos administradores do sistema acedido e ser tratado como incidente de segurança. (*zero trust: visibility*).
- A capacidade dos servidores iniciarem ligações de rede deve ser restringida, definindo, conforme seja adequado, aplicações autorizadas, protocolos autorizados, endereços de destino autorizados e bloqueando as restantes. As tentativas impedidas devem originar alarme aos administradores do sistema e ser tratado como um incidente de segurança.
- A utilização de recursos do sistema acima de 85% deve originar um alarme aos administradores do sistema e ser tratado como incidente de segurança. (*zero trust: visibility*)
- Os sistemas servidores devem ter ativo e atualizado *software* de proteção antivírus.
- Os sistemas servidor devem ter ativa uma *firewall,* que deverá estar configurada da forma a bloquear todo o trafego por defeito e permitir seletivamente o tráfego necessário à função do servidor.
- Os sistemas servidor não podem ser utilizados para navegação da Internet ou outras funções de posto de trabalho.

3.3. Atualização dos sistemas

- Os sistemas operativos e aplicações devem estar dentro do período de vida definido pelo fabricante e ter instaladas as atualizações de segurança recomendadas pelo fabricante.
- Os sistemas operativos e aplicações que sejam descontinuados pelo fabricante e deixem de ter atualizações de segurança, devem ser retirados de uso.

3.4. Passwords

- As *passwords* utilizadas nos serviços digitais da UMinho devem ser de utilização exclusiva nessas contas.
- As *passwords* não devem ser guardadas desprotegidas em suportes digitais ou físicos. As *passwords* guardadas em suportes digitais devem estar cifradas, as *passwords* em suporte físico devem guardar-se em local fechado de acesso restrito ao titular.
- As *passwords* devem ser longas[3], originais e improváveis. Uma frase com três palavras aleatórias, desconexas, com letras, números e símbolos, constituirá uma *password* forte.

3.5. Controlo de acessos à informação

- O acesso à informação deve ser controlado por intermédio de contas de utilizador individuais que permitam o rastreamento e responsabilização das ações de cada utilizador.
- A atribuição de privilégios de acesso a informação deve obedecer ao princípio do menor privilégio necessário e da segregação de funções.
- Os privilégios de acesso a informação devem ser permanentemente geridos, de acordo com os requisitos de confidencialidade dessa informação e a evolução da necessidade lhe aceder dos utilizadores de acordo com as suas funções a cada momento, acompanhando sem demora as alterações que sucedam.
- As contas sem utilização por período prolongado[4] deverão ser suspensas de modo automático.
- O mecanismo de autenticação deve bloquear o acesso à conta ao fim de algumas tentativas falhadas[5], para proteção de ataques do tipo força bruta. O bloqueio da conta deverá ser alertado aos administradores do sistema e ser tratado como um incidente de segurança em coordenação com o CSIRT.UMinho.
- O mecanismo de autenticação deve ser seguro, protegendo a confidencialidade e integridade da informação trocada.
- Sempre que os sistemas ou aplicações suportem autenticação multifator esta deve ser utilizada.

3.6. Interfaces de administração, consolas de execução de comandos e contas de privilégios elevados

- As contas de privilégios elevados devem ser pessoais e intransmissíveis, não devem ser partilhadas.
- A atribuição de privilégios elevados deve obedecer a um critério de necessidade estrita.
- A utilização de privilégios elevados, como perfis de "Administrador" e "Root", deve ser restrita a operações de instalação e configuração dos dispositivos.

---

[3] O número mínimo de carateres em passwords tem aumentado consecutivamente sendo 12 carateres a referencia atual, mas que aumentará com o passar do tempo.

[4] Utilize-se como referência para período prolongado 4 meses.

[5] Utilize-se 10 como referência para o número máximo de tentativas.

- O acesso a interfaces de administração, consolas de execução de comandos e privilégios elevados não deverá estar disponível da Internet, mas somente da rede interna da UMinho, localmente ou por VPN.
- O acesso a interfaces de administração, consolas de execução de comandos e privilégios elevados deve originar um alarme aos administradores do sistema.

3.7. Registos de utilização (logs)

- Os sistemas servidor deverão ter o relógio sincronizado com fonte oficial para coerência dos registos do conjunto de sistemas da UMinho.
- A informação mínima a constar dos registos de *log* deverá ser, conforme se aplique: data e hora, nome de utilizador, endereço e porto de origem e destino, protocolo, operação;
- Deve garantir-se a integridade dos *logs*, estabelecendo privilégios adequados de leitura, escrita e configuração e sempre que possível o envio de cópia dos logs para um sistema de *logging* centralizado. Nenhum utilizador deve poder desabilitar o registo das suas ações.
- Devem registar-se pelo menos os eventos de: autenticação; alterações a contas de utilizador; a utilização de privilégios elevados; a alteração da configuração da firewall, a tentativa de realizar operações bloqueadas, a exaustão de recursos do sistema;
- Os *logs* para a finalidade de segurança devem ter um histórico mínimo de 4 meses e máximo de 18 meses.
- Os *logs* de segurança são confidencias devendo estar acessíveis apenas aos administradores com responsabilidade pela segurança.

3.8. Cifragem / Segurança da informação

- A informação confidencial conservada em sistemas diretamente acessíveis da Internet deve ser conservada cifrada.
- A comunicação de informação confidencial deve ser cifrada.
- A comunicação de credenciais de acesso deve ser cifrada.

3.9. Cópias de segurança

- Toda a informação cuja perda constitua prejuízo para a UMinho deve ter pelo menos uma cópia de segurança periódica, preferencialmente automatizada.
- A informação em cópias de segurança deve estar sujeita a controlo de acessos não menos restrito que a informação original.
- Deve haver pelo menos uma cópia de segurança em dispositivo diferente da informação original. Esse dispositivo não poderá estar imediatamente acessível a partir do dispositivo original.
- A eficácia do processo que efetua as cópias de segurança deve ser verificada regularmente através da execução de testes de restauro.

4. Resposta a incidentes de segurança

- As notificações de segurança (alarmes) recebidas pelos administradores dos sistemas devem ser investigadas e tratadas.
- Um sistema que se suspeite estar comprometido deve ser imediatamente desconetado da rede, mas não deve ser desligado.
- Os incidentes de segurança informática devem ser reportados sem demora ao responsável da Unidade Orgânica / Serviço. O responsável da Unidade Orgânica / Serviço deve reportar os incidentes à equipa de resposta a incidentes de cibersegurança da UMinho (CSIRT.UMinho) para csirt@uminho.pt. Para proteger a integridade e/ou confidencialidade dos dados reportados, a mensagem pode ser assinada e/ou encriptada com recurso à chave PGP disponível em https://csirt.uminho.pt.
- Os incidentes de segurança informática devem ser investigados quanto à violação de dados pessoais. Essa investigação tem natureza urgente para que se possam tomar medidas de proteção dos titulares sem demora injustificada.
- As violações de dados pessoais deverão ser notificadas ao Encarregado da Proteção de Dados de acordo com as instruções constantes na página da Proteção de dados: https://www.uminho.pt/protecaodados.
- A notificação obrigatória de violações de dados pessoais à autoridade de controlo tem o prazo máximo de 72 horas desde que se conhece o incidente, pelo que as diligências junto do Encarregado da Proteção de Dados são urgentes.