**Proteção do Systema de Arquivos**

**1. Remoção do SUID Bit e do SGID Bit do Sestema**

O BIOS é um software básico, necessário para a inicialização da placa-mãe, responsável por

Nos UNIX-Like temos as tradicionais permissões **UGO (User, Group and Other)**. Para tornar as permissões mais flexíveis foram criadas mais três permissões especiais, que são as seguintes: SUID Bit, SGID Bit e Stick Bit.

A SUID Bit só pode ser aplicada em arquivos executáveis. Assim, o binário é executado com as permissões do dono e o SGID Bit quando é aplicado em um arquivo executável, funciona de forma parecida com o SUID Bit, mas é usada a permissão do grupo do arquivo. Além disso, esse bit pode ser aplicado em diretórios, quando isso acontece, tudo que for criado dentro desse diretório terá o grupo dele, ou seja, se o diretório pai tem o SGID Bit ativado, tudo que for criado dentro dele terá o seu grupo e não o do usuário que criou.

Como podemos ver o mais preocupante é o **SUID Bit**, já que, o binário será executado como usuário dono.

Por isso, o uso do **SUID Bit** deve ser limitado, já que isso pode implicar em falha de segurança. O **SUID Bit** quando aplicado em arquivos executáveis (já que o **SUID Bit** aplicado em diretório não tem efeito algum) faz com que este arquivo seja executado com as permissões do usuário dono do arquivo. Por exemplo, um usuário que execute um script que necessita gravar o log na pasta **/var/log** e este usuário não tem as permissões necessárias, poderemos usar o **SUID Bit** para que o usuário execute o script como se fosse o dono do script (por exemplo, como **root**) o qual tem as permissões necessárias de escrita no devido diretório.

**Conformidade com a Norma NBR ISO/IEC 27001:2013**

. Controle 001: Políticas para a segurança da informação.

5.1.1 - Convém que um conjunto de políticas de segurança da informação seja definido, aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes. (ABNT, NBR 27002, 2013, p.2).

. Controle 002: Análise crítica das políticas de segurança da informação.

5.1.2 - Convém que as políticas de segurança da informação sejam analisadas criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua continua pertinência, adequação e eficácia. (ABNT, NBR 27002, 2013, p.4).

. Controle 030: Gerenciamento de direitos de acesso privilegiados.

9.2.3 - Convém que a concessão e o uso de direitos de acesso privilegiado sejam restritos e controlados. (ABNT, NBR 27002, 2013, p.27).

. Controle 035: Restrição de acesso à informação.

9.4.1 – Convém que o acesso à informação e às funções dos sistemas de aplicações seja restrito, de acordo com a política de controle de acesso. (ABNT, NBR 27002, 2013, p.31).

. Controle 038: Uso de programas utilitários privilegiados.

9.4.4 - Convém que o uso de programas utilitários que podem ser capazes de sobrepor os controles dos sistemas e aplicações seja restrito e estritamente controlado. (ABNT, NBR 27002, 2013, p.33).

. Controle 061: Controles contra malware.

12.2.1 - Convém que sejam implementados controles de detecção, prevenção e recuperação para proteger contra malware, combinados com um adequado programa de conscientização do usuário. (ABNT, NBR 27002, 2013, p.51).

. Controle 078: Análise e especificação dos requisitos de segurança da informação.

14.1.1 - Convém que os requisitos relacionados à segurança da informação sejam incluídos nos requisitos para novos sistemas de informação ou melhorias dos sistemas de informação existentes. (ABNT, NBR 27002, 2013, p.67).

**2. Proteção do FileSystem**

Sempre que instalamos um sistema operacional Linux, devemos seguir a **FHS (FileSystem Hierarchy Standard)** e separar as partições que são compartilhadas para que possamos usar opções de montagem diferentes entre elas, além de nos proporcionar uma maior segurança.

Para inibirmos a utilização de forma arbitrária do uso do filesystem devemos definir alguma política de segurança em relação aos sistemas de arquivos montados. Isso pode ser feito utilizando algumas opções do comando **mount**, como foi feito no exemplo, atribuindo o **nosuid** na remontagem da partição ***/tmp***.

**Conformidade com a Norma NBR ISO/IEC 27001:2013**

. Controle 030: Gerenciamento de direitos de acesso privilegiados.

9.2.3 - Convém que a concessão e o uso de direitos de acesso privilegiado sejam restritos e controlados. (ABNT, NBR 27002, 2013, p.27).

. Controle 035: Restrição de acesso à informação.

9.4.1 – Convém que o acesso à informação e às funções dos sistemas de aplicações seja restrito, de acordo com a política de controle de acesso. (ABNT, NBR 27002, 2013, p.31).

. Controle 038: Uso de programas utilitários privilegiados.

9.4.4 - Convém que o uso de programas utilitários que podem ser capazes de sobrepor os controles dos sistemas e aplicações seja restrito e estritamente controlado. (ABNT, NBR 27002, 2013, p.33).

. Controle 061: Controles contra malware.

12.2.1 - Convém que sejam implementados controles de detecção, prevenção e recuperação para proteger contra malware, combinados com um adequado programa de conscientização do usuário. (ABNT, NBR 27002, 2013, p.51).

. Controle 078: Análise e especificação dos requisitos de segurança da informação.

14.1.1 - Convém que os requisitos relacionados à segurança da informação sejam incluídos nos requisitos para novos sistemas de informação ou melhorias dos sistemas de informação existentes. (ABNT, NBR 27002, 2013, p.67).

. Controle 109: Proteção de registros.

18.1.3 - Convém que registros sejam protegidos contra perda, destruição, falsificação, acesso não autorizado e liberação não autorizada, de acordo com os requisitos regulamentares, estatutários, contratuais e do negócio. (ABNT, NBR 27002, 2013, p.93).

. Controle 110: Proteção e privacidade de informações de identificação pessoal.

18.1.4 - Convém que a privacidade e a proteção das informações de identificação pessoal sejam asseguradas conforme requerido por legislação e regulamentação pertinente, quando aplicável (ABNT, NBR 27002, 2013, p.94).

**3. Proteção dos Arquivos de LOG**

Agora iremos proteger os logs do sistema usando o atributo de **append** do sistema de arquivos. Com isso, nossos logs não poderão ser apagados, reescritos e nem modificados, apenas novos registros poderão ser inclusos.

**Conformidade com a Norma NBR ISO/IEC 27001:2013**

. Controle 030: Gerenciamento de direitos de acesso privilegiados.

9.2.3 - Convém que a concessão e o uso de direitos de acesso privilegiado sejam restritos e controlados. (ABNT, NBR 27002, 2013, p.27).

. Controle 032: Análise crítica dos direitos de acesso de usuário.

9.2.5 – Convém que os proprietários de ativos analisem criticamente os direitos de acesso dos usuários a intervalos regulares. (ABNT, NBR 27002, 2013, p.28).

. Controle 035: Restrição de acesso à informação.

9.4.1 – Convém que o acesso à informação e às funções dos sistemas de aplicações seja restrito, de acordo com a política de controle de acesso. (ABNT, NBR 27002, 2013, p.31).

. Controle 038: Uso de programas utilitários privilegiados.

9.4.4 - Convém que o uso de programas utilitários que podem ser capazes de sobrepor os controles dos sistemas e aplicações seja restrito e estritamente controlado. (ABNT, NBR 27002, 2013, p.33).

. Controle 039: Controle de acesso ao código fonte de programas.

9.4.5 - Convém que o acesso ao código fonte de programas seja restrito. (ABNT, NBR 27002, 2013, p.34).

. Controle 061: Controles contra malware.

12.2.1 - Convém que sejam implementados controles de detecção, prevenção e recuperação para proteger contra malware, combinados com um adequado programa de conscientização do usuário. (ABNT, NBR 27002, 2013, p.51).

. Controle 063: Registro de eventos.

12.4.1 - Convém que registros (log) de eventos das atividades do usuário, exceções, falhas e eventos de segurança da informação sejam produzidos, mantidos e analisados criticamente, a intervalos regulares. (ABNT, NBR 27002, 2013, p.54).

. Controle 064: Proteção das informações dos registros de eventos (log).

12.4.2 - Convém que as informações dos registros de eventos (log) e os seus recursos sejam protegidos contra acesso não autorizado e adulteração. (ABNT, NBR 27002, 2013, p.55).

. Controle 065: Registro de eventos (log) de administrador e operador.

12.4.3 - Convém que as atividades dos administradores e operadores do sistema sejam registradas e os registros (log) protegidos e analisados criticamente, a intervalos regulares. (ABNT, NBR 27002, 2013, p.56).

. Controle 078: Análise e especificação dos requisitos de segurança da informação.

14.1.1 - Convém que os requisitos relacionados à segurança da informação sejam incluídos nos requisitos para novos sistemas de informação ou melhorias dos sistemas de informação existentes. (ABNT, NBR 27002, 2013, p.67).