Tópicos sobre o mecanismo de segurança do sistema operacional Windows

Augusto Henrique S R

Lucas F. Reinaldi

Cornélio Procópio, Brasil

***Abstract*—** **Information security is something that is necessary to implement in situations covered by the existing protection information of a particular company or person. Applying security both corporate information as the personal will Many great benefits. They should be established metrics for definer a security level, laying the foundation for analysis improvements. Security can be used in a framework of operating systems, operating the hardware, thus, its way of operating has to be safe to avoid bad intentioned people from stealing your personal data.**

***Keywords — Security, information Security, benefits of security windows security, user account control, bitlocker, applocker, windows defender.***

INTRODUÇÃO

A segurança da informação é um tópico que é necessário em várias situações que se referem à proteção existente sobre informações de uma determinada empresa ou pessoa. Aplicando segurança tanto a informações corporativas quanto a pessoais teremos otimos beneficios. Devem ser estabelecidas métricas para definer um nível de segurança, estabelecendo as bases para análise de melhorias. Segurança pode ser utilizado em um ambito de sistemas operacionais, operando o hardware, desta maneira, sua forma de operar tem que ser segura para evitar que pessoas má intencionadas roubem seus dados pessoais. No mundo atual, hackers tentam e podem acessar recursos e arquivos pessoais de diversos usuarios, causando danos para o mesmo. Além disso, muitas vezes os computadores compartilham informações confidenciais de empresas e pessoas importantes. Sendo assim, devem ser respeitados os protocolos de segurança.

Para que máquinas e usuários fiquem livres de problemas descritos acima, devemos implementar alguns tópicos de segurança em sistemas operacionais, cujo, devem estar sempre evoluindo. Há alguns tópicos a destacar, como autenticação de usuário, controle de acesso de arquivos, controle de contas para dividir permissões de acordo com caada usuário que utiliza a máquina. E um dos mais importantes, o gerenciamento de usuários.

Neste artigo, abordaremos algumas tecnologias relacionadas ao sistema operacional Windows voltadas a segurança de usuários.

Temos o AppLocker, como um controlador de aplicações que serão utlizados pelo usuário ou grupo de usuários em um sistema/rede. O AppLocker aceita regras e impõe elas sob o sistema, evitando ou permitindo usuários a manusear dados importantes. O BitLocker é uma medida de segurança do SO. O Bitlocker serve para garantir a integridade dos arquivos quando o sistema operacional não está ativo, ou seja, caso seja roubado uma máquina, quem a roubou não terá acesso facil aos dados, devido a encriptação de dados que o bitLocker ofere.

Em ultimo, temos o windows defender, que merece um certo destaque por ser um software de verificação, onde consegue encontrar e muitas vezes eliminar programas maliciosos que o usuário não sabe que existe ou não tem conhecimento para eliminá-los por conta.

TÓPICOS DE SEGURANÇA DO SISTEMA OPERACIONAL WINDOWS

Este tópico prega mencionar tópicos em relação a segurança de usuários que utilizam o Wndows como sistema operacional principal.

Estipulamos alguns conceitos de definições que serão usadas para o entendimento da seção a seguir.

*ACLs:* Listas de controle de acesso.

*ACEs:* Entradas de controle de acesso.

*Token: Determina aleatoriamente para o usuário códigos para acesso após a autenticação.*

*Autenticação de usuário*

A autenticação de usuários presa verificar e validar o usuário que acessa o sistema operacional, de um objeto ou de um serviço.

O mesmo checa sua genuinidade ao fazer uma solicitação que requer uma identidade própria permitida, fazendo com que apenas o usuário conheça ou possúa uma determinada para acessar o sistema. Por exemplo, biometria, uma senha, etc.

O fornecimento de uma autenticidade, normalmente vem por uma senha, que é criptografada por uma chave que apenas o usuário conhece e passa para o servidor, no qual terá uma chave criptográfica compartilhada ou pública que compara os dados para que seja verificada a autenticidade.

Serviços de domínio Active Directory do windows é uma tecnologia usada para armazenar informações de usuários, de maneira segura. O SO implementa uma boa quantidade de tecnologias capazes de armazenar informações e registos de usuários de maneira concreta, consisa e segura, tais como Kerberos, NTLM, SSL/TLS.

Além de implementar tecnologias capazes de garantir a segurança, existem protocolos que são combinações de pacotes com autententicações, como Credential Security Support Provider. Desta maneira, as tecnologias permitem um acesso seguro.

Citarei o kerberos como aplicação prática.

Kerberos será utilizado para autenticar um domínio do Active Directory.

Será implementado sistemas operacionais Windows Server, onde seus protocolos de autenticação serão Kerberos na versão 5,tendo extensões para autenticação de chaves públicas. Para que sejá autorizado a autenticação Kerberos, implementamos um provedor de suporte de segurança denominado SSP, podendo ser acessado pela interface SSPI.

A autenticação inicial é integrada a arquitetura de logon de um Winlogon. O certo de distribuição de Chaves Kerberos ficará integrado aos serviços de segurança do WS, executando o controlador de domínio usando banco de contas de segurança.

O Active Directory é exigido para implementar os kerberos que são padrões. [1]

*Controle de acesso*

Para controle de acesso, necessitamos de um processo de autorização de acesso definindo o controle de acesso ao usuário.

Este processo segue a partir de um momento em que o usuário ou grupo acessam um objeto, fazendo com que o seja passado ao subsistema de segurança do sistema operacional a verificação necessária. Se o token de acesso for permitido, será acessado tal objeto.

A verificação é concluida ao comparar as informações do token ao acesso do usuário, como as entradas do objeto (ACES)

As entradas de objeto denominadas ACEs teêm um comportamento diferente de acordo com cada objeto. Cada uma delas combinadas a um ACL, possuem um subsistema de segurança que verificará a ACL do objeto para os ACES, nos quais os usuparios estarão contidos para que seja verficada sua permissão sobre o objeto [2]

*Controle de conta de usuários*

Podemos criar e determinar usuários normais, sem serem de grupo de usuários administrador no windows.

Desta menira podemos ter usuários utilizando o sistema com privilégios limitados, evitando instalações de programas que não são devidos dentro do sistema, ou até mesmo, impedir que o usuário altere configurações impostas no sistema em que o mesmo está atuando.

Determinamos um modo de “Controle de Pais”, limitando acesso a filhos ( usuários) para criar um ambiente seguro. [3]

*Gerenciamento de usuários e domínios*

Podemos gerenciar o sistema operacional, baseando-se em usuários ou domínios de usuáriso que são grupos.

Cada computador possui um usuário administrador para que tenha acesso de como alterar, criar, ou remover um usuário. Estes uma vez determinados possuem menos acesso a recurssos e privilégios, podendo também, ter acesso limitado em determinado sistema ou nem executando arquivos.

Esta maneira é implementada com muita frequência em empresas e organizações, para que seja limitado recursos e por terem uma diversisade de usuário muito grande.

Cada tipo de usuário neste contexto forma um grupo para que cada grupo tenha permissão ou acesso de acodo com sua posição e necessidade.

Esta maneira de gerenciamento é facilitado utilizando o AppLocker, já explicado em tópciso acima.

TECNOLOGIAS DE SEGURANÇA DO SISTEMA OPERACIONAL WINDOWS

Nesta seção serão mencionadas algumas das tecnologias utilizadas em relação a segurança pelo sistema operacional

Windows.

*AppLocker*

App Locker é uma maneira de limitar usuários. Podendo controlar aplicativos, scripts, arquivos do Windows e até dlls.

Por meio dele podemos criar regras, aplicando exceções e limitados para grupos, oferencendo assim uma maneira de impedir ou garantir acesso à arquivos.

Utilizamos AppLocker para auditoria, como simulações de teste de controle sobre usuários. [3]

*BitLocker*

O BitLocker é utilizado quando o sistema operacional não está ativo (Offline). Estabelece medidas extras para proteger dados quando a proteção física é comprometida, como um roubo de máquina, por exemplo.

Temos maneiras de garantir esta segurança utilizando tecnologia como senha em BIOS para previnir acesso não autorizado.

O windows utiliza o BitLocker Drive Encryption que deixa encriptado informações e acesso em discos rígidos, tendo duas divisões: BitLocker Standard e BitLocker To Go.

O BitLocker Standard previni acesso não autorizado a dados em computadores perdidos ou roubados podendo encritar todo o sistema operacional Windows no disco rígido. Ou verificando integridade de componentes na inicialização

O modo Standard trabalha em conjunto com a Trusted Platform Module (TPM), uma tecnologia de criptografia. Implementando uma variedade de funções

Já o BitLocker To Go é bastante utilizado quando se trata de USB flash disks. Que são mais provenientes de serem roubados. O BTG encripta completamente os dispositivos USB flash disks que usam o sistema FAT.

De forma parecida com o BitLocker Standard, o BTG encripta o volume usando AES, a chave decodificadora é encriptada com múltiplas chaves protetoras e uma chave de recuperação pode ser salva em um arquivo. A diferença é que o BTG não utiliza as funcionalidades do TPM ou criptografia de chave pública. [4]

*Windows Defender*

O mais comumente utilizado por usuários leigos é o WD, que nada mais é de que um software que visa remoção de arquivos malíciosos que tentam acessar recursos e arquivos da máquina, como cavalos de tróia, malwares, adwares, spywares e vírus que estão presentes no computador.

O Windows defender ativado monitora a máquina prevenindo instalações indevidas de alguns arquivos maliciosos.

Possue atualização proveniente do Windows Update, tendo opções de acordo com seu propósito, oferecendo serviços desde varedura do sistema à controle de acesso/instalação de arquivos que causarão problemas à máqina. Monitorando as ações do usuário evitando problemas com arquivos máliciosos.

Como opções de registro, o usuário pode escolher os arquivos a serem excluídos, deixados em quarentena ou até mesmo deixar permitido para ser executado sem a interrupção ou bloqueamento pelo software.

Por fim, o software aparenta apenas encontrar software maliciosos para a plataforma Windows. [5]

REFERENCES

Nesta seção serão encontradas as referências utilizadas para a montagem deste artigo.

[1] Microsoft, acesso em Outubro de 2016. https://msdn.microsoft.com/pt­br/library/hh831472(v=ws.11).aspx [2] Microsoft, acesso em Outubro de 2016. https://technet.microsoft.com/pt­br/library/cc753976(v=ws.11).aspx [3] Chris Corio, “An introduction to security in Windows 7”.

[4] Mark E. Russinovich, David A. Solomon, Alex Ionescu,, “Windows Internals, part 2”, 2014.

[5] Xuxian Jiang, Xinyuan Wang, Dongyan Xu “Stealthy malware detection through vmm­based “out­of­the­box” semantic view reconstruction”.