

ARTIGO ORIGINAL

SILVA, Thiago Martins da ^[1]

SILVA, Thiago Martins da. Segurança da Informação em Servidores Linux: Um estudo de caso aplicado ao Bacula. Revista Científica Multidisciplinar Núcleo do Conhecimento. Ano 06, Ed. 02, Vol. 09, pp. 107-132. Fevereiro de 2021. ISSN: 2448-0959, Link de acesso: <https://www.nucleodoconhecimento.com.br/tecnologia/servidores-linux>

Contents

- RESUMO
- 1. INTRODUÇÃO
- 2. REFERENCIAL TEÓRICO
 - 2.1 SEGURANÇA DA INFORMAÇÃO E LINUX
 - 2.2 RESPOSTAS ÀS AMEAÇAS NA SEGURANÇA DA INFORMAÇÃO
 - 2.3 BOAS PRÁTICAS PARA A SEGURANÇA DA INFORMAÇÃO EM SERVIDORES LINUX
- 3. ESTUDO DE CASO APLICADO
 - 3.1 CARACTERIZAÇÃO DA EMPRESA
 - 3.2 CENÁRIO ATUAL
 - 3.3 PROPOSTA DE SOLUÇÃO
 - 3.3.1 A FERRAMENTA BACULA
 - 3.4 RESULTADOS OBTIDOS
- CONCLUSÃO
- REFERÊNCIAS

RESUMO

Os ataques cibernéticos estão causando estragos em empresas em todos os lugares. E, embora os ataques de hackers e *ransomware* certamente estejam causando danos e ganhando manchetes, *malware*, *spyware* e vírus antigos continuam sendo os principais motivos para violações de sistema e perda de dados. Com esses tipos de ameaças, não é uma questão de quando sua empresa se tornará uma vítima; é apenas uma questão de

quando o software anti-malware e antivírus pode ajudar. Ainda assim, mesmo com software de segurança atualizado, a maioria das empresas permanecem expostas à ameaças de perdas de dados devido a *hackers*, *malware* e *ransomware*. Com a prevalência significativa de servidores Linux em todo o mundo, a segurança é frequentemente apresentada como um ponto forte da plataforma para esse propósito. No entanto, um servidor baseado em Linux é tão seguro quanto sua configuração e, muitas vezes, são bastante vulneráveis a comprometimentos. Embora as configurações específicas variem enormemente devido aos ambientes ou uso específico, existem várias etapas gerais que podem ser executadas para garantir que as considerações básicas de segurança estejam em vigor. Desta forma, este artigo busca abordar sobre a importância dos sistemas de segurança da informação para servidores Linux, enfatizando o estudo através de uma aplicação de software Bacula, em um cenário problemático que não conta com um sistema eficiente de segurança, evidenciando o antes e o depois da aplicação.

Palavras Chaves: Servidores, Linux, Segurança, Sistema de Gestão, Bacula.

1. INTRODUÇÃO

Linux é o sistema operacional mais comumente usados para computadores voltados para a web, sendo executado em quase 75% dos servidores de acordo com os dados de agosto de 2019 da Netcraft. O Linux impulsiona a Internet como se conhece, ele dominou o mundo digital desde o início e não diminuiu desde então. É por isso que a segurança da informação em servidores Linux é crucial para a segurança dos dados (NETCRAFT, 2019).

Independentemente da plataforma de navegação para dispositivos moveis, por exemplo, o Linux provavelmente desempenha um papel importante em sua “vida” diária – mesmo que não se esteja totalmente ciente disso. Essa realidade fica ainda mais evidente no mundo dos negócios, onde o Linux é responsável pela presença na web de empresas de todos os portes. Na verdade, a pesquisa de junho de 2020 da Netcraft mostra que o Linux também alimenta nove dos sites das 10 empresas de hospedagem mais confiáveis (NETCRAFT, 2020).

A problemática desta pesquisa, resume-se nas preocupações com a segurança que são quase tão comuns quanto o próprio Linux. Esses servidores têm sido atacados há anos, mas

muitos usuários permanecem sem saber até que ponto seus dados podem ser comprometidos sem medidas proativas de segurança do servidor. Mas o que se pode fazer para proteger um servidor e aumentar a segurança do servidor Linux?

Desta forma, explora-se como objetivo principal a função de fortalecimento do Linux através de práticas que se pode colocar em ação imediatamente, evitando os ataques de usuários não autorizados a utilizarem dos recursos de sistema.

Esta pesquisa, justifica-se, pois muitos dos problemas de segurança do servidor Linux que se pode enfrentar ocorrem, em parte, porque eles não chegam protegidos de fábrica, ou seja, de suas distribuições nativas. Em vez disso, a responsabilidade é do usuário de configurar sistemas que revelem atividades suspeitas. Sem esse esforço extra, os servidores Linux podem ser extremamente vulneráveis. Assim sendo, as práticas relacionadas aqui, podem contribuir significativamente para se evitar este cenário, justificando mais uma vez o propósito desta pesquisa.

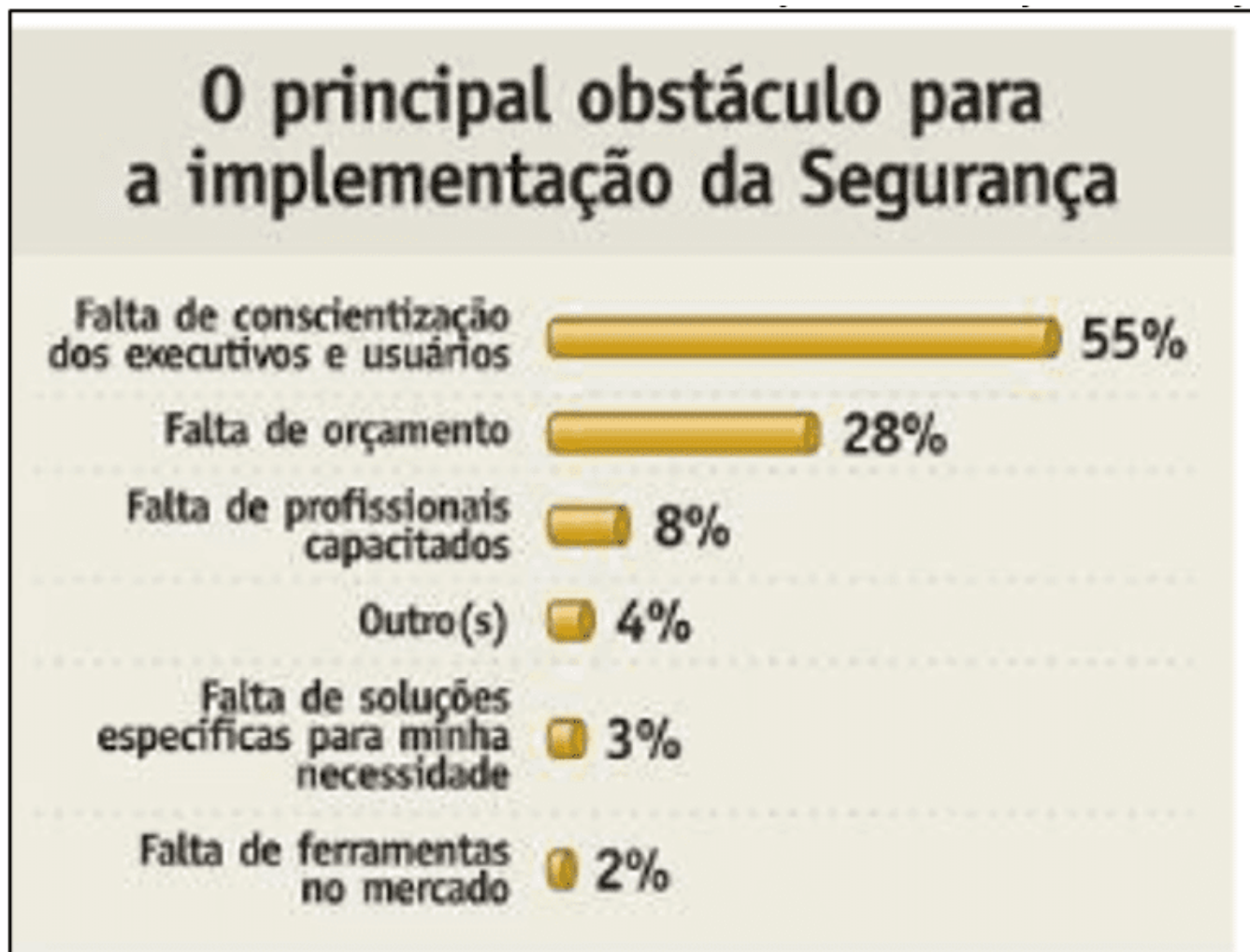
Para complicar ainda mais as coisas, muitas das principais iniciativas de segurança de hoje se concentram no *front office*, e não no *rack* do servidor. Isso fornece muitas oportunidades para que partes mal-intencionadas adquiram dados confidenciais e os resultados podem ser devastadores. Não há necessidade de adotar uma abordagem passiva e sucumbir às preocupações com a segurança do servidor Linux, um protocolo estratégico, focado na prevenção de riscos e na mitigação precoce, pode fazer toda a diferença.

2. REFERENCIAL TEÓRICO

2.1 SEGURANÇA DA INFORMAÇÃO E LINUX

A segurança da informação, preocupa-se com a proteção das informações contra acesso não autorizado (TITON, 2013). Faz parte do gerenciamento de risco de informações e envolve a prevenção ou redução da probabilidade de acesso não autorizado, uso, divulgação, interrupção, exclusão, corrupção, modificação, inspeção ou gravação. Na Figura 1, Titon (2013), enfatiza os principais obstáculos que os profissionais encontram para a implementação da Segurança da Informação.

Figura 1 – Principais obstáculos para a implementação de segurança da informação



Fonte: Titon (2013) – modelo adaptado pelo autor

Se um incidente de segurança ocorrer, os profissionais de segurança da informação estão envolvidos na redução do impacto negativo do incidente. As informações das notas podem ser eletrônicas ou físicas, tangíveis ou intangíveis. Embora o foco principal de qualquer programa de segurança da informação seja proteger a confidencialidade, integridade e disponibilidade (a tríade da CIA) das informações, a manutenção da produtividade organizacional costuma ser uma consideração importante (PEREIRA, 2014)

Isso levou a indústria de segurança da informação a oferecer orientação, políticas de segurança da informação e padrões da indústria sobre senhas, software antivírus, firewalls,

software de criptografia, responsabilidade legal e conscientização de segurança, para compartilhar as melhores práticas (JUNIOR, 2018).

Segundo, Junior (2018) a segurança da informação é alcançada por meio de um processo de gerenciamento de risco estruturado que:

- Identifica informações, ativos relacionados e as ameaças, vulnerabilidade e impacto do acesso não autorizado;
- Avalia riscos;
- Toma decisões sobre como abordar ou tratar os riscos, ou seja, evitar, mitigar, compartilhar ou aceitar;
- Quando mitigado, seleciona, projeta e implementa controles de segurança;
- Monitora atividades e faz ajustes para resolver quaisquer novos problemas, mudanças ou melhorias;

As ameaças à segurança da informação vêm em muitas formas, não se limitando a desastres naturais, mau funcionamento do computador ou servidor e roubo físico. Embora, ainda existam negócios baseados em papel, a dependência cada vez maior de sistemas de informação fez com que a segurança da informação se tornasse uma consideração chave no gerenciamento de riscos de segurança cibernética e aumentasse a necessidade de especialistas em segurança de TI dedicados (BARBOSA, 2012).

Esses profissionais de segurança de tecnologia da informação estão preocupados com a segurança de dados, segurança de aplicativos, segurança de rede, segurança de computador e segurança física. Entenda que os dados, aplicativos e computadores estão se espalhando muito além do que é tradicionalmente considerado um computador. Smartphones, mesas e outros dispositivos móveis são tão parecidos com um computador quanto um servidor ou mainframe e são suscetíveis a ataques cibernéticos maliciosos que podem obter acesso a informações confidenciais, informações críticas, ativos de informação ou controle de sistemas informáticos internos importantes (DAWEL, 2005).

Isso, junto com o aumento da quantidade de violações de dados, levou a uma maior demanda por planejamento sofisticado de proteção de dados e a uma crescente demanda por profissionais de segurança cibernética para entenderem a segurança da informação. Um número crescente de certificações de segurança da informação está disponível e os empregadores geralmente preferem funcionários com certificações que validem os conhecimentos das melhores práticas.

Existem amplas certificações, como o *Certified Information Systems Security Professional* (CISSP), e outras específicas que cobrem garantia de informações, segurança de rede, testes de segurança, auditoria de negócios, planejamento de continuidade de negócios, testes de segurança, planejamento de resposta a incidentes, roubo de identidade, avaliações de risco, intrusão sistemas de detecção, violações de segurança e todas as outras medidas de segurança (FONTES, 2006).

As funções comuns que exigiam experiência em gerenciamento de informações incluem diretor de segurança de TI (CSO), diretor de segurança da informação (CISO), engenheiro de segurança, analista de segurança da informação, administrador de sistemas de segurança e consultor de segurança de TI. Desta forma, mais pessoas do que nunca estão preferindo usar o Linux. Embora o Windows e o MacOS ainda capturem a maior parte do mercado, quase 2% de todos os computadores usam o sistema operacional (FONTES, 2006).

Embora isso possa não parecer muito, a parcela de uso cresceu imensamente nos últimos anos. Enquanto apenas 2% dos computadores desktop usam os sistemas operacionais, 96,5% dos milhões de domínios principais do mundo são movidos por servidores Linux (JIRASEK, 2012).

Mas o Linux é mais seguro do que o MacOS e o Windows? De certa forma, sim. Mas isso não significa que tenha suas vulnerabilidades. Aprender sobre a segurança da informação no Linux e como pode-se proteger independentemente da distribuição que usar, é um passo importante para uma boa gerência de dados. A maneira mais fácil de melhorar a segurança cibernética, independentemente do sistema operacional, é com uma VPN (Rede Virtual Privada). As VPN's protegem a conexão com a Internet e ocultam o endereço IP (Protocolo de Internet). Embora não proteja contra malware, aumenta sua privacidade.

As ameaças podem vir de várias formas, incluindo ataques de software, roubo de identidade, sabotagem, roubo físico e extorsão de informações. Os ataques de software à segurança da informação incluem vírus, *malware* (software malicioso, qualquer programa ou arquivo prejudicial ao usuário do computador), *worms* (um tipo de software malicioso que se autorreplica, infectando outros computadores enquanto permanece ativo nos sistemas infectados.) *ransomware* (um tipo de software malicioso, ou malware, projetado para negar acesso a um sistema de computador ou dados até que o resgate seja pago. O ransomware se

espalha através de e-mails de *phishing*, visitando sites infectados ou explorando vulnerabilidades.) como WannaCry ou cavalos de Tróia (JIRASEK, 2012).

E-mails ou sites de *phishing* costumam ter como objetivo roubar propriedade intelectual ou credenciais de login para obter acesso não autorizado. A engenharia social é uma das maiores ameaças cibernéticas e é difícil de se proteger com as medidas de segurança tradicionais (MOREIRA, 2001).

A sabotagem, como ataques de negação de serviço, muitas vezes visa reduzir a disponibilidade de ativos de informações importantes, reduzindo a confiança ou a produtividade organizacional até que um pagamento seja recebido em troca da devolução do serviço à organização. O roubo de informações e equipamentos está se tornando cada vez mais comum, já que a maioria dos dispositivos agora são de natureza móvel, como *smartphones* ou *laptops*.

A extorsão de informações envolve obter acesso a informações confidenciais e, em seguida mantê-las como resgate até que o pagamento seja feito. Há muitas maneiras de se proteger contra ataques cibernéticos, mas a ameaça número um a qualquer organização são seus usuários ou funcionários internos, que são suscetíveis a engenharia social ou *phishing*. É por isso que o treinamento de conscientização sobre segurança cibernética e os controles de segurança são importantes em todos os níveis da uma organização.

2.2 RESPOSTAS ÀS AMEAÇAS NA SEGURANÇA DA INFORMAÇÃO

Segundo Pinheiro (2007), quando uma ameaça é identificada, normalmente tem-se uma escolha:

- Reduza ou mitigue o risco implementando salvaguardas ou contramedidas para eliminar ou reduzir ameaças e vulnerabilidades;
- Atribuir ou transferir o risco para outra entidade ou organização por meio da compra de seguro ou terceirização;
- Aceitar o risco quando o custo da contramedida for maior do que o possível custo de perda devido a uma vulnerabilidade ou ataque cibernético;

Com a introdução do Regulamento Geral de Proteção de Dados (GDPR) pelo Parlamento Europeu e o Conselho em 2016, a necessidade de responder às violações de segurança da informação tornou-se um requisito regulamentar para qualquer empresa que opere na UE. No Brasil a LGPD (2018), Lei Geral de Proteção de Dados, que entrou em vigor em 2018, menciona que as empresas agora são obrigadas a:

- Fornecer notificações de violação de dados;
- Nomear um oficial de proteção de dados requer consentimento do usuário para processamento de dados;
- Anonimizar dados para privacidade;

Isso torna um plano abrangente de tratamento de incidentes e detecção de vazamento de dados um requisito para a maioria das empresas globais.

Existem muitas maneiras de definir a segurança da informação, mas tanto o Instituto Nacional de Padrões e Tecnologia (NIST) e o Glossário de Garantia da Informação Nacional (IA) definem segurança da informação como a proteção da informação e dos sistemas de informação contra acesso não autorizado, uso, divulgação, interrupção, modificação ou destruição para fornecer confidencialidade, integridade e disponibilidade (NIST, 2020).

Desta forma, o (NIST, 2020), ainda menciona que em resposta as ameaças à segurança da informação, é preciso aplicar, conforme já mencionado anteriormente a Confidencialidade (confidencialidade consiste em não disponibilizar ou divulgar informações a indivíduos, entidades ou processos não autorizados. Embora sejam semelhantes à privacidade, as palavras não devem ser usadas alternadamente), integridade (integridade de dados preocupa-se com a manutenção, garantia, precisão e durante todo o seu ciclo de vida. Isso significa implementar controles de segurança que garantam que os dados não possam ser modificados ou excluídos por uma pessoa não autorizada ou de maneira não detectada.) e disponibilidade (para que qualquer sistema de informação seja útil, ele deve estar disponível quando necessário. Isso significa que os sistemas de computador que armazenam e processam informações, os controles de segurança que as protegem e os canais de comunicação que as acessam devem funcionar sob demanda.), também conhecidas como a tríade da CIA, estão no cerne da segurança da informação.

Dito isso, há um debate sobre se a tríade da CIA atende ou não suficientemente às rápidas

mudanças de tecnologia e requisitos de negócios, bem como a relação entre segurança e privacidade. Outros princípios, como responsabilidade, foram propostos e o não repúdio não se encaixa bem com os três conceitos centrais.

O gerenciamento de risco da informação é o processo de identificação de vulnerabilidades e ameaças aos recursos de informação usados por uma organização e se alguma contramedida deve ser tomada para reduzir o risco a um nível aceitável com base no valor da informação para a organização (LAUREANO, 2002).

Existem duas considerações principais com qualquer processo de gerenciamento de risco, onde (LAUREANO, 2002), menciona que:

- O processo de gestão de risco é contínuo e de natureza interativa, deve ser repetido indefinidamente à medida que novas ameaças e vulnerabilidades surgem;
- A escolha de contramedidas ou controles usados deve atingir um equilíbrio entre produtividade, custo, eficácia e o valor da informação do ativo que está sendo protegido;

A análise e avaliação de risco têm limitações inatas porque, quando ocorrem incidentes de segurança, eles surgem no contexto e podem vir de ameaças imprevisíveis ou inesperadas, como *buckets S3* (uma das soluções líderes de armazenamento em nuvem, é usada por empresas em todo o mundo para uma variedade de casos de uso para potencializar suas operações de TI) mal configurados ou invasores externos (MITINIK e SIMON, 2003).

A probabilidade de uma ameaça usar uma vulnerabilidade para causar danos cria riscos. No contexto da segurança da informação, o impacto é a perda de confidencialidade, integridade ou disponibilidade ou todas as outras perdas possíveis (por exemplo, danos à reputação e financeiros). Nota: Não é possível identificar nem mitigar todos os riscos. Este risco remanescente é denominado risco residual (MITINIK e SIMON, 2003).

As avaliações de risco cibernético são definidas pelo NIST (2020) como avaliações de riscos são usadas para identificar, estimar e priorizar o risco para as operações organizacionais, ativos organizacionais, indivíduos, outras organizações e a nação, resultante da operação e uso de sistemas de informação. Em um alto nível, uma avaliação de risco cibernético envolve uma auditoria de dados que responde:

- Que dados coletamos?
- Como e onde estamos armazenando esses dados?
- Como protegemos e documentamos os dados?
- Por quanto tempo mantemos os dados?
- Quem tem acesso interno e externamente aos dados?
- O local onde armazenamos os dados está devidamente protegido? Muitas violações vêm de *baldes S3* mal configurados, sendo preciso verificar permissões do S3.

E então define-se os parâmetros da avaliação:

- Qual é o objetivo da avaliação?
- Qual é o escopo da avaliação?
- Existem prioridades ou restrições das quais devo estar ciente que podem afetar a avaliação?
- A quem preciso acessar na organização para obter todas as informações de que preciso?
- Qual modelo de risco a organização usar para análise de risco?

Desta forma, ressalta-se que uma vulnerabilidade, é uma fraqueza ou exploração que pode causar danos, perda ou exposição a um ativo de informação (NAKAMURA e GEUS, 2007). Uma “fraquez” no sistema, ou um “exploit”, pode ser considerado um pedaço de software, dado ou sequência de comandos que se aproveita de uma vulnerabilidade para causar comportamento não intencional ou para obter acesso não autorizado a dados confidenciais (NAKAMURA e GEUS, 2007).

Assim que as vulnerabilidades são identificadas, elas são publicadas em Vulnerabilidades e Exposições Comuns (CVE). CVE é um dicionário de vulnerabilidade gratuito projetado para melhorar a segurança cibernética global e a resiliência cibernética, criando um identificador padronizado para uma determinada vulnerabilidade ou exposição (NAKAMURA e GEUS, 2007).

2.3 BOAS PRÁTICAS PARA A SEGURANÇA DA INFORMAÇÃO EM SERVIDORES LINUX

Embora proteger os servidores Linux possa parecer um incômodo, o processo vem com uma fresta de esperança: ele fornece um grau extra de controle. Além do mais, a segurança do servidor não é necessariamente difícil de alcançar. Segundo (NAKAMURA e GEUS, 2007)

algumas práticas recomendadas básicas de proteção do Linux e segurança do servidor Linux podem fazer toda a diferença, conforme explana-se a seguir:

Usar senhas fortes e exclusivas: Senhas fortes formam a base de qualquer servidor seguro. Se possível, eles devem apresentar um comprimento mínimo de pelo menos 10 caracteres, além dos requisitos para o uso de caracteres especiais ou letras maiúsculas e minúsculas. A mesma senha nunca deve ser usada para vários usuários ou sistemas de software. Não se esqueça de configurar a expiração, pois nenhuma senha pode fornecer segurança adequada indefinidamente. Vários gerenciadores de senhas excelentes estão disponíveis para a plataforma Linux. Muitos deles oferecem recursos essenciais, como:

- Autenticação de dois fatores,
- Geradores de senha;
- Armazenamento de senha em nuvem.

Bitwarden, LastPass, Enpass e Dashlane representam algumas das melhores opções disponíveis. No entanto, nenhum gerenciador de senhas é ideal para todos os servidores; portanto, é importante examinar suas opções minuciosamente para garantir que se encontre uma abordagem personalizada que atenda suas necessidades exclusivas.

Gere um par de chaves SSH: Embora as senhas fortes possam fazer a diferença, métodos ainda mais eficazes de login em servidores privados estão disponíveis. Os pares de chaves Secure Shell (SSH), em particular, valem a pena implementar porque esses sistemas são muito mais difíceis de hackear com força bruta. Antes de utilizar as chaves SSH, é importante entender por que se pode querer implementá-las em vez da configuração padrão de nome de usuário e senha. Embora as senhas sejam certamente mais convenientes para usuários comuns, esses mesmos usuários tendem a confiar em opções facilmente adivinhadas que deixam toda a infraestrutura de segurança vulnerável. Os pares de chaves SSH, embora não sejam tão amigáveis quanto às senhas, são significativamente mais seguros. Essa segurança aprimorada pode ser atribuída à criptografia utilizada pelo servidor que está sendo conectado e pelo computador que está sendo usado. No mínimo, um par de chaves SSH representa o equivalente a uma senha de 12 caracteres. Na realidade, entretanto, a grande maioria dos pares de chaves SSH são ainda mais complexos. Por esse motivo, os pares de chaves SSH devem ser uma das primeiras medidas implementadas ao adotar uma estratégia de segurança proativa do servidor.

Atualizar os softwares regularmente: O gerenciamento adequado da segurança do servidor Linux inclui uma implementação de patches regulares de software para lidar com vulnerabilidades emergentes. Infelizmente, muitos usuários do Linux negligenciam colocar esses patches em ação. Sem atualizações imediatas, o software pode se tornar explorável e fácil de ser usado por hackers para obter acesso. Uma grande variedade de opções permite que se atualize o Linux enquanto usa o Ubuntu (uma das distribuições do Linux), por exemplo. Isso inclui linhas de comando e o Gerenciador de atualizações do Ubuntu.

Ative as atualizações automáticas: Essa prática recomendada anda de mãos dadas com a última sugestão para maior segurança do servidor Linux. Se tem dificuldade em lidar com uma infinidade de atualizações de segurança necessárias, considere a implementação de uma abordagem automática. Habilitar atualizações automáticas garante que as medidas de segurança do software permaneçam atualizadas, mesmo quando se esquece de buscar as atualizações necessárias porque está ocupado com outras preocupações.

Evite software desnecessário: Um novo software pode ser tentador de implementar, mas nem todos os serviços da Web são realmente necessários. Cada programa adicional oferece mais uma oportunidade de expor o servidor a problemas potenciais no futuro. Embora seja tentador adicionar um software novo e empolgante quando estiver disponível pela primeira vez, essa abordagem pode levar a consideráveis preocupações de segurança a longo prazo. Com o tempo, mesmo os sistemas mais eficientes podem ficar atolados e inchados por causa de programas não utilizados, impraticáveis ou redundantes. É aconselhável fazer uma auditoria de todo o sistema de todo o software pelo menos uma vez por ano. Ao assumir esse compromisso simples, se pode otimizar o servidor e mantê-lo funcionando com eficiência máxima, mesmo ao adicionar novos programas.

Desative a inicialização de dispositivos externos: Pessoas mal-intencionadas podem facilmente usar dispositivos externos, como pen drives USB, para obter acesso a informações confidenciais. A inicialização desabilitada para dispositivos externos pode reduzir o potencial de ataques físicos, que podem ser tão prejudiciais quanto hackers. Sem essa etapa extra, muitas camadas de segurança podem ser facilmente contornadas.

Fechar as portas abertas ocultas: Portas abertas podem revelar informações de arquitetura de rede enquanto estendem as superfícies de ataque. Portanto, as portas que não são

absolutamente essenciais devem ser fechadas com pressa. O comando *netstat* pode ser usado para determinar quais portas estão escutando enquanto também revela os detalhes das conexões que podem estar disponíveis atualmente. Os exemplos de linhas de comando abaixo podem ser utilizados para encontrar portas específicas:

- Todas as portas TCP – “netstat -at”
- Todas as portas UDP – “netstat -au”
- Todas as portas de escuta – “netstat -l”
- Informações para todas as portas – “netstat -s”

Verificar arquivos de log com Fail2ban: Ataques de força bruta são surpreendentemente comuns com servidores Linux. No entanto, eles geralmente são bem-sucedidos não porque as partes mal-intencionadas sejam particularmente capazes ou desonestas, mas, sim, por causa da pura falta de medidas preventivas além da proteção de senha ligeiramente melhorada. Se está procurando uma solução de próximo nível para evitar ataques de força bruta, considere a implementação do software de prevenção de intrusão *Fail2ban*. Este sistema altera as regras do *firewall* para proibir qualquer endereço que tenha tentado fazer login um determinado número de vezes. Ele pode ser usado para detectar e resolver padrões de falha de autenticação. Os alertas de e-mail fornecem avisos imediatos de ataques para garantir que o servidor seja controlado o mais rápido possível.

Utilize backups e teste-os com frequência: Os backups externos são essenciais para servidores Linux. No caso de uma intrusão, eles podem garantir que os dados críticos permaneçam acessíveis. Eles são particularmente valiosos no caso de um ataque de *ransomware*. Embora eles não possam impedir completamente os problemas de *ransomware*, eles podem garantir que, no pior cenário, o dano seja limitado pela retenção do acesso aos dados essenciais. O aplicativo *rsync* é uma opção popular para fazer backup de dados no Linux. Ele vem com uma série de recursos que permitem fazer backups diários ou impedir que determinados arquivos sejam copiados. É notoriamente versátil e, portanto, uma ótima opção para uma vasta gama de estratégias de segurança de servidor Linux.

Realizar auditorias de segurança: Embora as sugestões destacadas acima possam fornecer mais paz de espírito enquanto se esforça para melhorar a segurança do servidor Linux, ameaças adicionais podem estar ao virar da esquina. Mesmo o servidor mais seguro eventualmente se tornará vulnerável a novos perigos se não for atualizado regularmente. As

atualizações de software são cruciais, é claro, mas as auditorias de segurança podem revelar outros ajustes que valem a pena. Sem auditorias regulares, é impossível saber onde existem lacunas ou como elas podem ser resolvidas para garantir que o servidor permaneça totalmente protegido.

3. ESTUDO DE CASO APLICADO

3.1 CARACTERIZAÇÃO DA EMPRESA

A empresa LOJAS MUNDO M.E, hoje localizada no município de Goiânia, estado de Goiás, pode ser considerada como uma empresa recente, criada por um Ex-Coordenador de Sistemas de Informação e por sua esposa que possui formação em Administração de Empresas e especialização em Gestão de Pessoas. Apesar do proprietário ter profundos conhecimentos na área de T.I, atuando como professor / educador e coordenador de cursos técnicos, o mesmo se desligou e resolveu investir em uma área totalmente diferente da qual estava acostumado a atuar.

Mesmo sem domínio desta nova área, ou seja, artesanatos e moveis em MDF no geral (produtos industrializados), sua família possui antecedentes com histórico na fabricação de móveis a mais de 50 anos na mesma cidade de atuação da empresa. A esposa por sinal, possui profundo conhecimento na área, e além de administrar os negócios, também trabalha na personalização de todos os itens em MDF e artesanatos em geral que a empresa possui.

Em 2015, a empresa foi construída com um capital inicial de um pouco mais de 50 mil reais, e não possuía funcionários diretos em seu quadro empregatício, ou seja, na mesma trabalham um casal (proprietários) que estão à frente de todas as rotinas da empresa.

Por ser considerada uma empresa pequena, constituída como microempresa, mediante informações colhidas através dos proprietários, em um futuro próximo a intenção é contratar no mínimo três funcionários para atuar com a parte de designer das peças (construção dos projetos) e dois vendedores diretos dentro da empresa. Atualmente a empresa trabalha com um sistema de emprego indireto terceirizando vários serviços de personalização, devido ao grande volume de pedidos em pouco tempo de existência.

A empresa realiza compra dos produtos de várias regiões do Brasil, busca e preza sempre pela qualidade dos seus produtos além de garantir ao cliente um resultado satisfatório. Sua divulgação é focada em mídias sociais, onde através da internet, consegue levar seus produtos a um número considerado de clientes, que estão sempre à procura pelos produtos.

A empresa hoje, foca muito no segmento de móveis para festas em geral, lembrancinhas para eventos em geral, além da personalização dos itens dispostos em várias técnicas de artesanato, pintura, entre outros.

A empresa é totalmente focada no ramo comercial e possui como atividade principal a compra e venda de peças em MDF no geral, além do recorte personalizado de peças feitas a laser, empregabilidade de técnicas de personalização nas peças da loja como pintura, verniz, craquelamento, envelhecimento da madeira, decoupage com papéis especializados, encapagem com tecidos, rendas, fitas, resinas, apliques de madeira de uma forma geral.

Através das tendências que vão ditando o ritmo em uma série de segmentos, com o artesanato não é diferente, apesar da empresa estar a pouco tempo no mercado, a mesma participa de feiras de artesanato, levando seu produto para o estado de São Paulo.

Além de ter um consumo local pela população através de Kit's Higiênicos para recém-nascidos, lembrancinhas para várias ocasiões (nascimento, batizados, casamentos, formaturas), brindes para empresas, além dos móveis vendidos para comerciantes locais que trabalham diretamente com festas e eventos que demandam de cenários personalizados com temas específicos, serviços de plotagem, entre outros.

Figura 2 - Produtos personalizados pelo LOJAS MUNDO M.E



Fonte: Próprio autor

A empresa busca através do crescimento no segmento, diversificar Kits higiênicos (conforme figura 02 acima), dando opções aos clientes de personalizações diferenciadas (ao gosto do cliente) através de temas para qualquer tipo de ocasião, no caso da imagem acima o tema foi Safari.

Normalmente a empresa LOJAS MUNDO M.E possui outros concorrentes diretos e indiretos na cidade de Goiânia-GO. Várias livrarias e papelarias da cidade trabalham com MDF (algumas opções) promovendo a concorrência. Na mesma rua onde a loja é situada, possui outra empresa que trabalha no segmento de personalização de itens em MDF (principalmente na linha infantil), além de outras empresas na cidade que também atua no mesmo segmento, porém a empresa hoje é especializada na área, e conta com um catálogo de produtos vasto, conseguindo atender boa parte da demanda local e cidades próximas.

O fato da empresa atender vários clientes através das mídias sociais e também por recursos móveis como WhatsApp, ajudam a manter um atendimento constante, além de proporcionar

através das imagens, orçamentos, desenhos realizados no Corel, uma visão da prospecção da peça, ajudando o cliente nos processos de decisão.

A estratégia adotada, é de analisar o tipo de serviço/produto oferecido pelas demais empresas, identificando quais as melhores oportunidades de diferencia-se perante os clientes. Este é o ponto forte da estratégia, uma vez que a correta escolha de fornecedores/produtos somados à excelência técnica e de atendimento, tornam a relação pessoal (Comunicação verbal) um ponto positivo na divulgação da empresa.

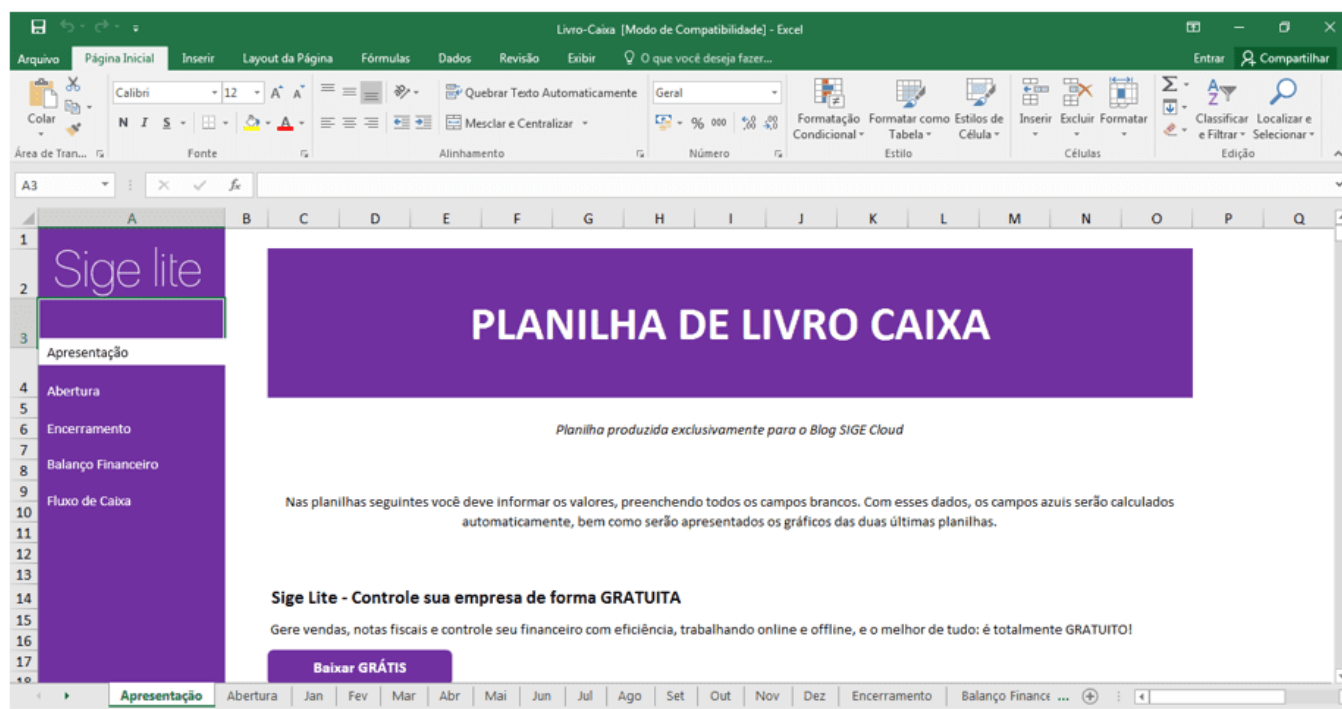
A chamada propaganda “boca a boca” através dos clientes satisfeitos torna-se muito eficaz neste mercado, além de baixo custo. Existem também campanhas de marketing disseminando os novos “valores da empresa”.

3.2 CENÁRIO ATUAL

Atualmente a empresa possui um software para o gerenciamento das rotinas internas da empresa. Os proprietários mediante reunião relataram a dificuldade de se registrar as ações e rotinas da empresa, onde, apesar do proprietário possuir amplo conhecimento em técnicas e gerenciamento de T.I, optou-se pela terceirização do serviço devido ao comprometimento do mesmo com as ações da empresa.

Ambos sabem que atualmente a empresa precisa fornecer relatórios técnicos sobre seus clientes, fidelização, controle de estoque, caixa, etc., ou seja, o sistema da empresa é baseado em livros caixa desenvolvido no Excel para informações básicas, porém há necessidade não só de um gerenciamento mais aprofundado das rotinas, mas também faz-se necessário armazenar todas as informações relativas aos seus clientes, fornecedores, produtos, catálogos de peças personalizadas, e os proprietários não possuem um sistema de segurança que possa gerenciar tais processos. As planilhas que gerenciam as operações da empresa são disponibilizadas gratuitamente através do portal (<https://www.sigelite.com.br/>).

Figura 3 – Planilha de Controle de Caixa – SigeLite



Fonte: SIGELITE, 2020. Modelo Adaptado.

O sistema é bem simplificado e carece de várias informações gerenciáveis no qual a empresa necessita para uma melhor compreensão dos processos e gerenciamento das rotinas internas da empresa. Por não possuir um banco de dados para o registro das informações, a empresa fica a “mercê” de uma planilha simplificada, onde são registradas as informações básicas do dia a dia da empresa. Deste modo, não é possível realizar um controle adequado das informações principalmente mediante das necessidades dos proprietários.

Porém, segundo os proprietários, eles pretendem investir em um sistema personalizado no futuro, mas a necessidade de se manter os arquivos atuais em um sistema mais confiável e prioridade, necessitando assim de um mecanismo automático para realização de cópias programadas de segurança de todas as informações da empresa.

Atualmente a empresa conta com 1 servidor com sistema operacional em Linux e 3 estações de trabalho e consulta dentro da loja possuindo sistema operacional Windows 10. Segundo os proprietários, a necessidade de armazenar várias informações diariamente, e mesmo com o conhecimento do proprietário, o mesmo mencionou ferramentas gratuitas em Linux, porém à necessidade de se terceirizar o serviço mediante sua rotina de trabalho.

3.3 PROPOSTA DE SOLUÇÃO

Mediante cenário acima, evidenciado para este estudo de caso, fica claro que a empresa LOJAS MUNDO M.E, está praticamente no início de suas atividades comerciais, mesmo que a “família” tenha vários anos de experiência no seguimento.

A falta de sistema personalizado para o gerenciamento das rotinas, e evidente, porém a empresa atualmente conta com um sistema simplificado (SIGE), que consegue atualmente atender a demanda. O grande problema é a falta de um sistema de cópia (backup) das informações para o servidor Linux que a empresa possui, garantindo assim a possível restauração das informações em caso de acidentes.

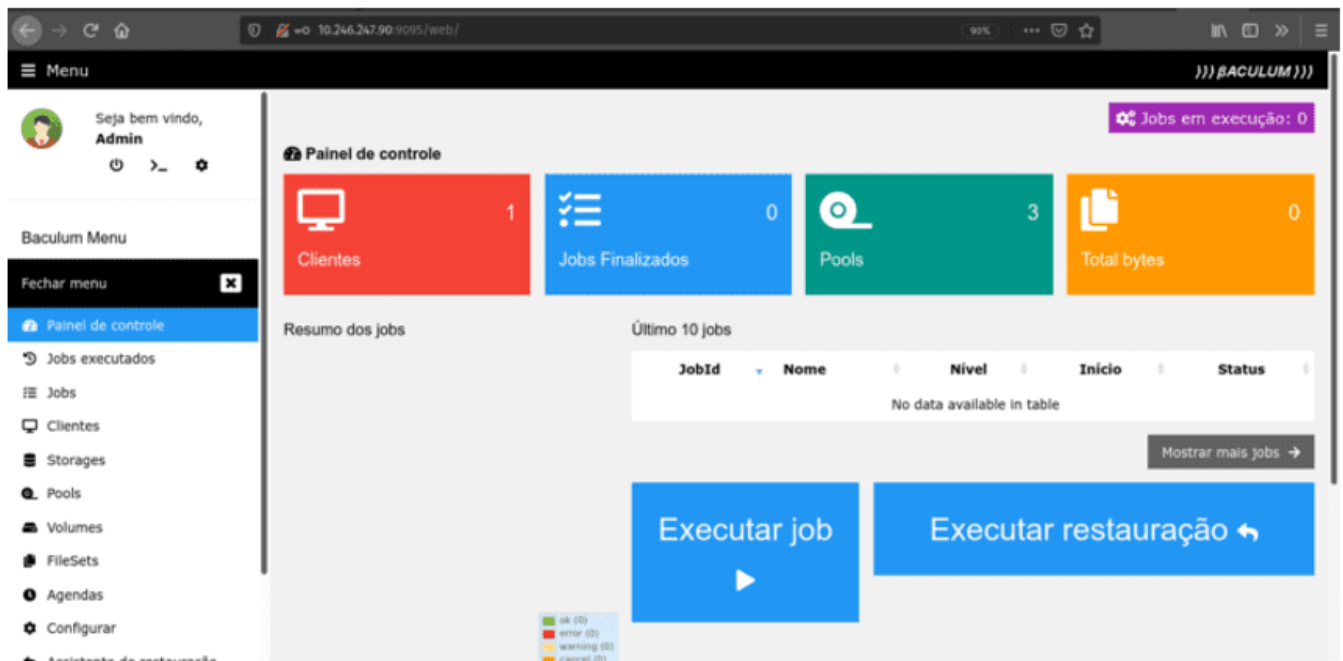
Desta forma, este autor, propôs como solução, a instalação e configuração da ferramenta Bacula para sistema operacional Linux, resolvendo assim os problemas relacionados a falta de backup das informações da empresa.

3.3.1 A FERRAMENTA BACULA

Desde o início de seu desenvolvimento, o Bacula foi construído como um sistema de backup baseado em Linux nativo. A adequação do Linux como sistema operacional central tanto para o desenvolvimento quanto para o uso de uma solução de backup empresarial tornou-o o sistema operacional básico escolhido pelo Bacula (SILVA, 2015).

Bacula é uma solução ágil pronta para a empresa, capaz de fazer backup e restaurar dados no menor tempo possível (SILVA, 2015). Bacula tem a reputação de ser um software de backup Linux extremamente flexível, seguro e gratuito e, até o momento, teve mais downloads do que qualquer outro software de backup Linux de código aberto. Ele oferece suporte a uma ampla variedade de tipos de backup – de backup físico a virtual e em nuvem que oferece suporte ao Amazon S3 (BACULABRASIL, 2020). Ele também oferece mais flexibilidade no lado do armazenamento, integrando-se com discos, e uma ampla variedade de unidades de fita. Bacula é conhecido por funcionar perfeitamente bem com drivers de fita SCSI em máquinas FreeBSD, Linux, Solaris e Windows. A Figura 04 abaixo mostra bem o ambiente amigável do Bacula para Linux.

Figura 4 – Ambiente Bacula para Linux



Fonte: CORREA, 2020. Modelo Adaptado pelo autor.

Bacula usa sua ampla gama de ferramentas e habilidades para fazer backup, proteger e restaurar grandes quantidades de dados baseados em Linux. Surpreendentemente, o Bacula como sistema é amigável e altamente personalizável – na verdade, pode ser considerado uma das soluções de backup mais personalizáveis disponíveis em qualquer lugar.

Chevarriam e Luz (2012), relatam alguns dos benefícios de usar o software de backup e restauração Bacula como sua solução de backup para sistemas baseados em Linux:

- Uma ampla variedade de níveis e técnicas de backup possíveis, incluindo completo, diferencial, incremental, completo virtual e muito mais;
- Capacidade de fazer backup e restaurar sistemas inteiros ou arquivos únicos com apenas alguns cliques ou comandos de console;
- Suporte de backup em nuvem para S3;
- Capacidade de usar snapshots em sistemas Linux / Unix. Instantâneos podem ser criados automaticamente e usados para fazer backup de arquivos. Também é possível gerenciar Snapshots a partir da ferramenta console do Bacula por meio de uma interface única;
- Use a linha de comando e / ou GUI para executar e controlar seu processo de backup;
- Use o backup de partição para seus armazenamentos de dados Linux para manter imagens precisas desses discos para fácil gerenciamento e recuperação;

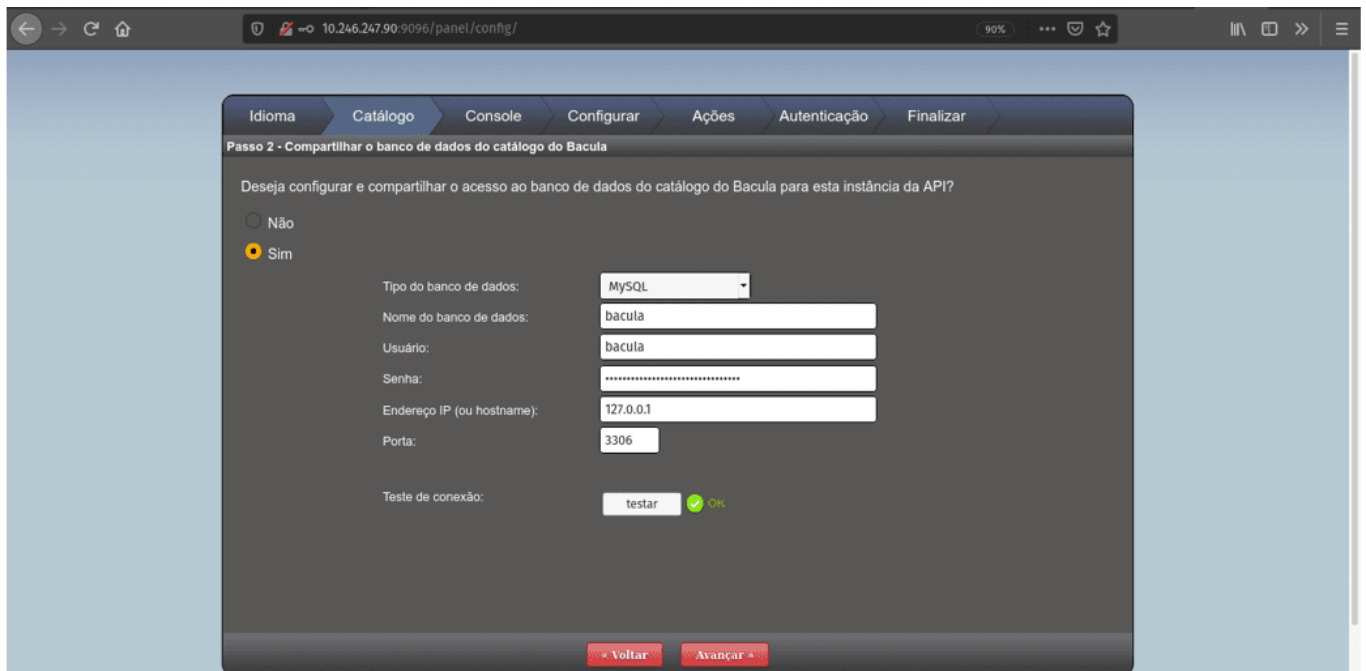
Bacula, como um software de backup Linux gratuito, funciona com a maioria das variações populares de distribuições Linux, incluindo Debian, Ubuntu, CentOS, RedHat e muito mais. Seu desenvolvimento e design de código aberto permitem que a solução como um todo funcione bem com quase todos os sistemas baseados em Linux com desempenho e estabilidade (CHEVARRIAM e LUZ, 2012). Um exemplo é o backup de bancos de dados como PostgreSQL e MySQL – o backup e a restauração são realizados com velocidade e facilidade, combinados com controle granular sobre os dados (MENDES, 2004).

Segundo a BACULABRASIL (2020), a variedade e complexidade dos recursos do Bacula como uma solução de backup Linux gratuita permite uma ampla variedade de todos os tipos de recursos, incluindo:

- O backup em fita é totalmente suportado pelo Bacula e permite trabalhar com uma variedade de diferentes drives de fita, auto carregadores e autochangers. O suporte VTL também está incluído. Bacula também oferece suporte para fita WORM.
- Como um software de backup Linux de código aberto, Bacula oferece suporte a backups de vários volumes
- Um banco de dados padrão SQL completo e abrangente de todos os arquivos de backup. Isso significa que a visualização online pode ser feita de arquivos salvos em qualquer volume particular.
- A deduplicação de volumes alinhados é um tipo de deduplicação de dados desenvolvido pela Bacula que é rápido e eficiente. Ele otimiza de forma inteligente o posicionamento dos arquivos para que um sistema de arquivos de deduplicação subjacente (ZFS, por exemplo) possa deduplicar de forma otimizada os dados de backup gravados pelo Bacula.
- Atualmente existem drivers para MySQL, PostgreSQL e SQLite. Qualquer mecanismo de banco de dados SQL pode ser usado, portanto, o backup dos bancos de dados SQL pode ser feito com confiabilidade e velocidade.
- A opção de usar o Baculum como uma alternativa GUI intuitiva para trabalhar diretamente com um console Linux.
- A recuperação *baremetal* permite a recuperação fácil do sistema desde o início até o último ponto de backup. Isso é quase sempre automatizado para sistemas Linux e pode ser usado como parte de uma estratégia de recuperação de desastres. Um CD de resgate para sistemas Linux também está disponível
- Faça backup de uma ampla variedade de dados de máquina virtual, como VMware, Red Hat, Hyper-V, KVM e muito mais. Colocar um daemon de arquivo Bacula na máquina virtual permite que você restaure os dados da máquina virtual com um alto nível de controle.
- Automatizar as operações de backup e restauração também está disponível no Bacula como parte de sua ampla personalização, como agendador, script, manutenção de tarefas e assim por diante.
- O backup em nuvem com Bacula é capaz de funcionar com Amazon e S3.

O Bacula atualmente está na versão 9.6.7, sendo um lançamento para a correção de alguns bugs da versão anterior. Abaixo, denota-se um dos processos de instalação do Baculum (interface mais amigável para Linux).

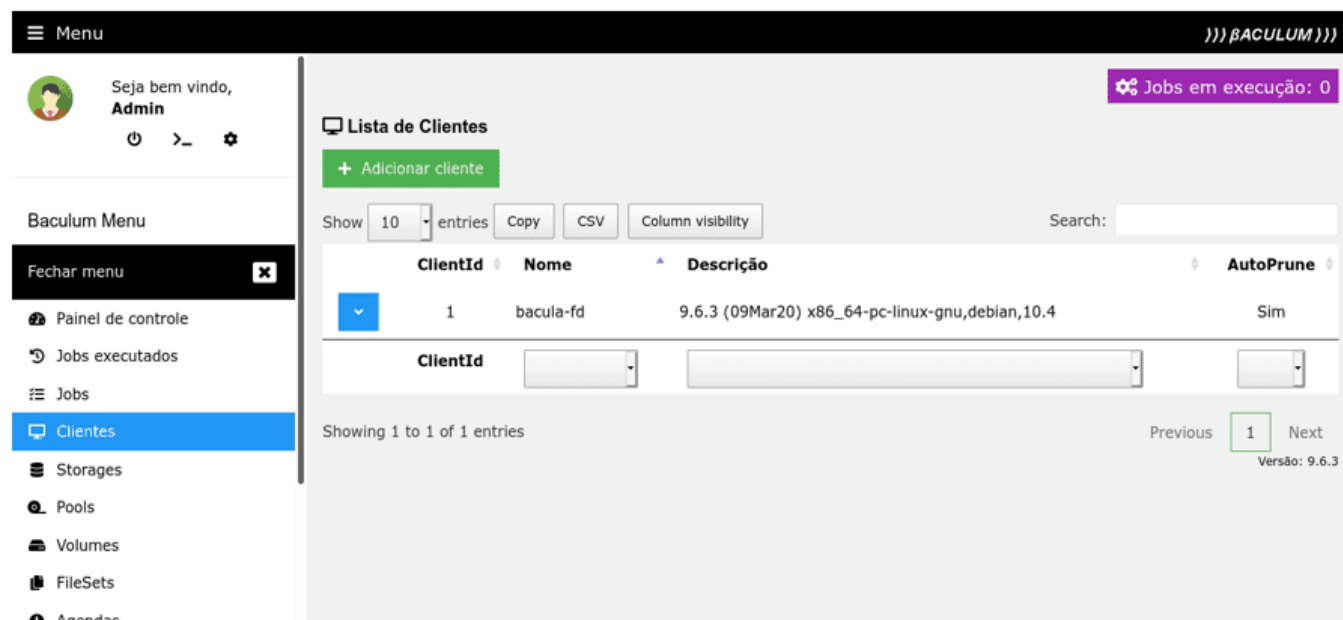
Figura 5 – Interface de Instalação do Baculum



Fonte: BACULABRASIL, 2020. Modelo Adaptado pelo autor.

Na Figura 06 abaixo, é possível observar o ambiente de configuração dos clientes de backup do Bacula. É possível configuração vários clientes de backup com localizações diferentes de arquivos, hora, data, permissões, etc.

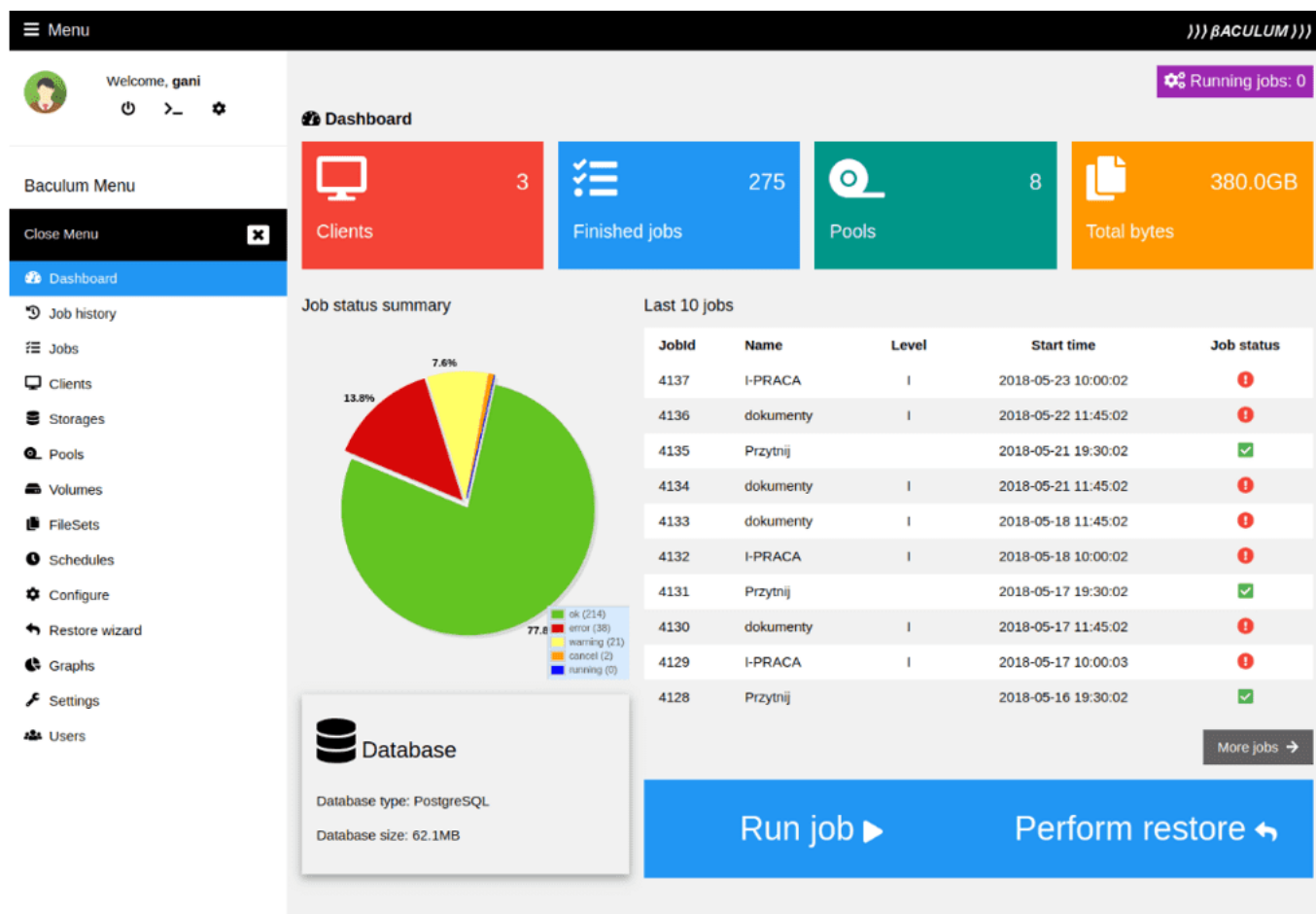
Figura 6 Gerenciador de Clientes para Backup do Bacula



Fonte: BACULABRASIL, 2020. Modelo Adaptado pelo autor.

Segundo a comunidade do Bacula no Brasil, as novas interfaces do sistema de backup estão mais intuitivas, amigáveis e totalmente integradas com a WEB. É perfeitamente possível obter rapidamente vários relatórios das cópias realizadas pelos “clientes”, no servidor.

Figura 7 Relatório de cópias realizado no Bacula



Fonte: BACULABRASIL, 2020. Modelo Adaptado pelo autor.

3.4 RESULTADOS OBTIDOS

Com a implantação do Bacula, atualmente a empresa LOJAS MUNDO M.E, pode contar com um sistema robusto, devidamente configurado para realizar cópias de segurança diariamente, ao final do expediente, com arquivos datados, tanto em servidor local, ou seja, no Linux, como um espelhamento dos dados para as nuvens também.

Um fator importante, que diferencia o Bacula dos outros softwares de backup, é o fato de por padrão o Bacula decide quais arquivos fazer backup para backup incremental e diferencial comparando os tempos de alteração (*st_ctime*) e modificação (*st_mtime*) do arquivo com a hora do último backup concluído. Se uma dessas duas vezes for posterior à hora do último

backup, será feito o backup do arquivo. No entanto, isso não permite rastrear quais arquivos foram excluídos e perderá qualquer arquivo antigo que possa ter sido restaurado ou movido para o sistema de arquivos do cliente.

Outro ponto observado durante os testes, aplica-se sobre a diretiva *Accurate* = *<yes | no>*, sendo que se estiver habilitada (padrão não) no recurso *Job*, o *job* será executado como um *Job Accurate*. Para um backup completo, não há diferença, mas para backups diferenciais e incrementais, o servidor enviará uma lista de todos os arquivos anteriores de backup e o *daemon* de arquivo usará essa lista para determinar se novos arquivos foram adicionados ou movidos e se algum arquivo foi excluído. Isso permite que o Bacula faça um backup preciso do sistema até aquele ponto no tempo para que, se fizer uma restauração, ele restaure o sistema exatamente conforme os últimos dados coletados. Uma nota de cautela sobre o uso do backup preciso, é que ele requer mais recursos (CPU e memória) nas máquinas do servidor e do cliente para criar a lista de arquivos de backup anteriores, para enviar essa lista para o *daemon* de arquivo, para manter a lista (possivelmente muito grande) na memória, e para o *daemon* de arquivo fazer comparações entre cada arquivo no *FileSet* e a lista.

Vale ressaltar que, se estiver usando um programa como *TAR*, *DUMMP* ou *BRU* para fazer backup dos dados do computador e desejar uma solução de rede com mais flexibilidade ou serviços de catálogo, o Bacula provavelmente fornecerá os recursos adicionais que deseja.

No entanto, se for novo em sistemas Unix ou não tiver um pouco de experiência compensadora com um pacote de backup sofisticado, este autor não recomenda o uso do Bacula, pois é muito mais difícil de se configurar e usar do que os programas *TAR* ou *DUMP*. Se desejar que o Bacula se comporte como os programas simples mencionados acima, e escreva sobre qualquer fita de backup que se colocar no drive, então provavelmente usuários menos experientes terão dificuldade em trabalhar com este mecanismo de segurança com Bacula.

O Bacula foi projetado para proteger os dados seguindo as regras que o administrador de rede especificar, e isso significa reutilizar uma fita apenas como último recurso. É possível forçar o Bacula a escrever sobre qualquer fita na unidade, mas, é mais fácil e mais eficiente usar um programa mais simples para esse tipo de operação. Se quiser um programa de backup que possa gravar em vários volumes (ou seja, não limitado pela capacidade da

unidade de fita), o Bacula provavelmente pode atender as necessidades.

Além disso, vários usuários do Bacula relatam que o Bacula é mais simples de configurar e usar do que outros programas equivalentes. Se estiver usando um pacote comercial sofisticado como o Legato *Networker*, *ARCserveIT*, *Arkeia* ou *PerfectBackup* +, pode-se estar interessado no Bacula, que oferece muitos dos mesmos recursos, e é um software gratuito, disponível sob a licença de software *Affero GPL* Versão 3.

Com todas estas ressalvas e diretrizes, o estudo de caso, comprovou que o sistema é eficiente e promove sim, um controle adequado para cópias e restauração de dados com eficiência para pequenas e grandes empresas. É claro que existem soluções para cada tipo de situação, e também suporte exclusivo do Bacula para grandes corporações, onde uma equipe oferece suporte para cada tipo de cenário.

CONCLUSÃO

Relatórios de software malicioso e hackers estão por toda parte atualmente. E, embora esses tipos de ameaças representem riscos significativos para as empresas, certamente não são os únicos que existem. Portanto, com isso em mente, este artigo abordou sobre algumas das coisas que ameaçam os dados de uma empresa, e também a necessidade de se ter um bom sistema de backup, como o Bacula, citado neste estudo.

Bacula é um programa de backup, restauração e verificação e não é um sistema de recuperação de desastres completo em si, mas pode ser uma parte fundamental de um, se você planejar cuidadosamente e seguir instruções que se adequam aos mais tipos de cenários variados que se possa imaginar, baseando-se na própria documentação do Bacula, ou em comunidades conforme citada neste artigo.

Com planejamento adequado para recuperação de desastres, o Bacula pode ser um componente central do seu sistema de recuperação de desastres. Por exemplo, se criou um disco de inicialização de emergência e / ou um disco *BaculaRescue* para salvar as informações de particionamento atuais do seu disco rígido e mantém um *Baculabackup* completo, é possível recuperar completamente o seu sistema do "*bare metal*" que é começando a partir de um disco vazio. Se você usou o gravador *WriteBootstra* em seu

trabalho ou algum outro meio para salvar um arquivo de *bootstrap* válido, você poderá usá-lo para extrair os arquivos necessários (sem usar o catálogo ou pesquisar manualmente os arquivos para restaurar).

Vale mencionar que o Bacula é um conjunto de programas de computador que permite ao administrador do sistema gerenciar backups, recuperação e verificação de dados de computador em uma rede de computadores de diferentes tipos. O Bacula também pode ser executado inteiramente em um único computador e pode fazer backup em vários tipos de mídia, incluindo fita e disco. Em termos técnicos, é um programa de backup de rede baseado em cliente / servidor. Bacula é relativamente fácil de usar e eficiente, ao mesmo tempo que oferece muitos recursos avançados de gerenciamento de armazenamento que facilitam a localização e recuperação de arquivos perdidos ou danificados. Devido ao seu design modular, o Bacula é escalonável de pequenos sistemas de computador único a sistemas que consistem em centenas de computadores localizados em uma grande rede.

Simplificando, um backup de dados é apenas uma cópia dos arquivos do seu computador ou dispositivo. E, conforme ilustrado com as inúmeras ameaças descritas neste artigo, manter um backup de seus arquivos e dados de negócios importantes é essencial por vários motivos importantes. Praticamente todos os especialistas em informática e tecnologia dirão que qualquer backup é melhor do que nenhum. No entanto, nem todos os dispositivos e tecnologias de backup são iguais; nem todos oferecem os mesmos níveis de proteção.

Uma das maneiras mais fáceis de criar backups de dados corporativos é simplesmente armazenar cópias de arquivos importantes em discos rígidos, unidades de fita ou outros dispositivos de armazenamento conectados aos seus sistemas ou rede. Copiar arquivos para discos rígidos, unidades flash USB, unidades externas ou outros dispositivos conectados a sistemas individuais ou dispositivos conectados por meio de uma rede local ou de longa distância é uma forma eficaz de garantir que os backups estejam disponíveis localmente quando você precisar deles.

Com qualquer bom plano de recuperação de dados, manter cópias locais dos backups é essencial. No entanto, devido aos riscos associados a desastres físicos, ransomware, roubo e outras ameaças, manter backups locais nunca deve ser a única faceta de sua estratégia. Além de manter backups locais atualizados de seus arquivos e dados, você deve sempre

armazenar pelo menos uma cópia fora do local, ou seja, um servidor de backup externo ou na nuvem.

REFERÊNCIAS

BACULABRASIL (2020) Novo Design Baculum Bacula Community. Disponível em: <https://www.bacula.la/novo-design-baculum-bacula-community/> Acesso em: 31 dez. 2020.

BARBOSA, Felipe Santos. *Fundamentos em Segurança e Hardening em Servidores Linux baseado na Norma ISO 27002*. In: Anais do V ENUCOMP 2012, Parnaíba, PI 12 a 14 de novembro de 2012: FUESPI, 2012.

BRASIL (2018). LGPD - Lei Geral da Proteção de Dados. Lei nº 13.709, de 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato20152018/2018/lei/L13709.htm Acesso em: 21 dez. 2020.

CHEVARRIAM, Rafael V., LUZ, Ângelo G. da. Segurança da informação: Backup e o uso do Bacula. Faculdade de Tecnologia - Serviço Nacional de Aprendizagem Comercial (SENAC) - 2012 - Caixa Postal 96.015 -560 - Pelotas - RS - Brasil. Disponível em: http://187.52.54.51/wiki2012_2/lib/exe/fetch.php?media=projeto21:rafael_-_chevarria_-_backup_e_o_uso_do_bacula.pdf Acesso em: 31 dez. 2020.

CORREA, Lenon. Solução de backup completa Open Source: Bacula Community 9.6.x e Baculum 9.6.x. Disponível em: <https://blog.remontti.com.br/4460>. Acesso em: 31 dez. 2020.

DAWEL, George. A segurança da informação nas empresas. Rio de Janeiro: Editora Ciência Moderna Ltda., 2005.

FONTES, Edison Luiz Gonçalves. Segurança da informação: o usuário faz a diferença. São Paulo: Saraiva, 2006.

JIRASEK, Vladimir. *Practical application of information security models Original Research*

Article. Information Security Technical Report, Volume 17, Issues 1-2, February 2012, Pages 1-8

JUNIOR, Dorival M. M. Segurança da informação: uma abordagem sobre proteção da privacidade em internet das coisas. Pontifícia Universidade Católica de São Paulo PUC-SP, 2018.

LAUREANO, Marcos Aurélio P. Sistemas para Identificação de Invasão. Curso de Informática Aplicada – PUC-PR. Curitiba, PR, 2002.

MENDES, Sandro R. Montando um completo servidor de backup usando Bacula. Comunidade Viva Linux – 2004. Disponível em: <https://www.vivaolinux.com.br/artigo/Montando-um-completo-servidor-de-backup-usando-Bacula> Acesso em: 31 dez. 2020.

MITNICK, Kevin D.; SIMON, William L. A Arte de Enganar – ataques de hackers: controlando o fator humano na segurança da informação. São Paulo: Pearson Education do Brasil Ltda, 2003

MOREIRA, Nilton Stringasci. Segurança Mínima: uma visão corporativa da segurança de informações. Rio de Janeiro: Axcel Books, 2001.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício de. Segurança de Redes em Ambientes Cooperativos. São Paulo: Novatec, 2007.

NETCRAFT (2020). *Most Reliable Hosting Company Sites in June 2020*. Disponível em: <https://news.netcraft.com/archives/2020/07/02/most-reliable-hosting-company-sites-in-june-2020.html>. Acesso em: 21 dez. 2020.

NETCRAT (2019) *August 2019 Web Server Survey*. Disponível em: <https://news.netcraft.com/archives/2019/08/15/august-2019-web-server-survey.html>. Acesso em: 21 dez. 2020.

NIST (2020). *Information Security*. Disponível em: https://csrc.nist.gov/glossary/term/information_security Acesso em: 21 dez. 2020.

PEREIRA, Aline. Segurança da informação, conceitos e mecanismos. 2014. Disponível em: http://www.simensen.br/aulasvirtuais/material/9729_unidade_ii_com%C3%A9rcio.pdf. Acesso em: 21 dez. 2020.

PINHEIRO, José M. Dos Santos. Ameaças e Ataques aos Sistemas de Informação: Prevenir e Antecipar. Cadernos UniFOAedição nº 05, dezembro 2007. Disponível em: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwip482T5d_tAhXGGbkGHQ8fCncQFjABegQIBxAC&url=http%3A%2F%2Frevistas.unifoa.edu.br%2Findex.php%2Fcadernos%2Farticle%2Fdownload%2F885%2F790&usg=AOvVaw3sjtriVIMZ9cSMxuOgV6cO Acesso em: 21 dez. 2020.

SIGELITE (2020) Sistema de controle comercial personalizado. Disponível em: <https://www.sigelite.com.br/>. Acesso em: 31 dez. 2020.

SILVA, Ednilson Tondo da. Software livre no monitoramento de serviços e backup de dados por meio de redes de computadores. Universidade Tecnológica Federal do Paraná – departamento acadêmico de Informática – especialização Em Redes De Computadores, 2015. Disponível em: http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/5903/1/PB_ESPRC_II_2015_04.pdf Acesso em: 31 dez. 2020.

TITON, Regis. Segurança da informação aplicada a servidores utilizando técnicas de *hardening*. Universidade Federal De Santa Maria – Colégio Agrícola De Frederico Westphalenpós-Graduação Em Gestão De Tecnologia Da Informação, 2013. Rio Grande do Sul. Disponível em: https://repositorio.ufsm.br/bitstream/handle/1/249/Titon_Regis.pdf?sequence=1&isAllowed=y Acesso em: 21 dez. 2020.

^[1] Cursando o 5ª Período em Sistema da Informação Universidade Veiga de Almeida (UVA) e Cursando o 8ª Período em Engenharia da Computação Unicarioca.

Enviado: Janeiro, 2021.

Aprovado: Fevereiro, 2021.