Pensando Fora da Caixa

Monitorando a segurança DB2 no z/OS

Por Jerry Harding
Stephen D. Rubin
William Buriak

VitalSigns SIEM Agent™ for z/OS

WHITE PAPER

SUMÁRIO

1. Sumário Executivo 3
2. Background 4
3. O custo da violação de segurança dos dados 5
3.1 Responsabilidade Pessoal 5
3.2 Os Reguladores Cometh 5
4. A Exposição de Segurança Real ao DB2 no z/OS 6
5. Fraquezas no código do DB2 6
6. Utilizando Registros SMF do DB2 no Rastreamento de Eventos 7
7. implementando registros de auditoria do SMF no DB2 8
8. Pensando "Fora da Caixa" 9
8.1 Gerenciamento de logs 10
8.2 Produtos SIEM com suporte ao DB2 10
8.3 Soluções Próprias de Mainframe para o DB2 10
9. Sumário: 11
Sobre os autores: 13
Sobre A SDS 13

1. SUMÁRIO EXECUTIVO

Os Estados Unidos introduziram há alguns anos um sistema universal de saúde. Este sistema exigiu que os registros altamente sensíveis fossem armazenados em muitos computadores. Essencialmente, eles seriam como um "rastro de DNA" para milhões de Americanos. A segurança desses registros não deveria ser pensada “após o fato” e exigiria monitoramento vigilante e proativo da segurança, independentemente do sistema operacional.

Os registros devem ser protegidos de acordo com as normas federais, da Lei de Gerenciamento de Segurança da Informação de 2008 (FISMA, também conhecido como Projeto de lei do Senado dos EUA S.3474). O FISMA exige que “a estrutura de sistemas e ativos de informação dependam do processamento, transmissão, recebimento ou armazenamento de informações eletronicamente”, incluindo a segurança adequada. E continua: “Significando segurança proporcional ao risco e magnitude dos danos causados pela perda, uso indevido ou acesso não autorizado ou a modificação de informações”.

As conexões Web aos dados do DB2 no mainframe, através do Web Services do z/OS, CICS e TSO®, incluíram funcionalidades no processamento do legado e levaram o processamento de transações a novos patamares. Isso também introduziu uma nova percepção de vulnerabilidade. Os administradores da Segurança de Mainframe, por vezes, enxergam isso como uma brecha do mainframe para "Intrusos".

Esses "Intrusos" estão encontrando novas maneiras de obter informações pessoais e corporativas de forma a acarretar danos aos negócios de uma empresa, como aconteceu no sequestro de registros médicos do estado da Virgínia, onde foi exigido um resgate de US$ 10 milhões.

A maioria das indústrias financeiras, de saúde e farmacêuticas mantém seus registros vitais no DB2 e outros bancos de dados do z/OS da IBM. Os interesses do governo nessas empresas levam a próxima onda de troca de informações entre elas, e espera-se que empresas privadas que compartilhem informações de bancos de dados com o governo cumpram as diretrizes do FISMA.

Contudo, independentemente do setor e se eles se enquadram ou não nos regulamentos FISMA, toda empresa corre o risco de sofrer com a perda de informações. A segurança, por vezes, não é a maior prioridade em uma corporação até que isso seja matéria de destaque no noticiário da noite do Wall Street Journal, ou sua organização seja convocada a prestar esclarecimentos perante o Congresso.

1 Suas informações médicas valem de 10 a 20 vezes mais que o número do seu cartão de crédito no mercado negro, de acordo com um relatório de 2014 da Reuters.

Este artigo concentra-se em maneiras de monitorar a segurança do banco de dados DB2 do z/OS, pensando *fora da caixa*. O objetivo é oferecer alternativas para o desenvolvimento de um estrutura de segurança para monitorar configurações de segurança e proteger dados confidenciais de 'Intrusos' de maneira eficaz e econômica. Este artigo também explora as ferramentas disponíveis para desenvolver a estrutura da segurança. O foco principal está nas ferramentas que podem ser usadas fora da estrutura do mainframe. A ênfase em “pensar fora da caixa” é enfatizada como a maioria das ferramentas que se enquadram na configuração de segurança do mainframe, mas que não atendem os requisitos de segurança, auditoria e conformidade exigidos atualmente. Aqui também serão detalhadas as etapas a serem tomadas ao configurar a coleta de logs e programas de análise de segurança no mainframe, usando fontes econômicas e prontamente disponíveis. No entanto, além de mencionar a eficiência deste sistema, este documento também enfatizará a necessidade de um novo quadro, visto que muitas vezes as medidas

tradicionais são incapazes de combater as ameaças à segurança. Por fim, discutirá a métodos que podem ser adotados para combater as ameaças mais recentes e como essas ferramentas funcionam.

2. BACKGROUND

As equipes de segurança do DB2 no z/OS, geralmente usam produtos de segurança da IBM e da CA para gerar relatórios, e que acabam servindo como os primeiros níveis de proteção. Esses produtos permitem ou negam o acesso de um usuário a um recurso. Diferente da segurança do UNIX e de outros sistemas operacionais, ele é uma simples decisão de 'sim ou não'. Se negado, um evento de violação será gravado nos arquivos de log de segurança e, na maioria dos casos, uma mensagem será emitida para o console principal.
O evento pode passar despercebido até que o Administrador do sistema execute um relatório de violação em resposta a um incidente.

O DB2 é capaz de manter um arquivo de log separado de eventos durante o curso normal de processamento. Esses arquivos de log são uma função do sistema operacional de mainframe chamada System Management Facility ou "SMF®". Os registros SMF do DB2 contêm informações relacionados a diferentes tipos de eventos que ocorrem dentro do sistema. O nível de granularidade depende das configurações da trilha de auditoria do DB2 no nível da tabela individual.
Os registros SMF fornecem dados úteis para investigar eventos de segurança e, se usados em combinação com outros recursos, ajuda a investigar possíveis ataques e violações de resposta a incidentes, auditoria e conformidade. Os registros SMF do DB2 são criados em formato binário e não são legíveis por um editor de texto simples, fazendo com que a visualização on-line e a sua interpretação seja quase impossível.

Separação de Tarefas

Um dos aspectos mais fundamentais da Lei Sarbanes-Oxley de 2002 foi a definição de 'Separação de Tarefas'. Ter uma mesma pessoa monitorando a segurança e ao mesmo tempo configurando a segurança é um caso claro de violação da lei.

A Função de Segurança em Evolução

Os Administradores de Segurança na maioria dos ambientes z/OS são responsáveis pelo monitoramento da segurança. Além de definir e manter usuários e senhas, eles assumem a função de buscar relatórios para responder a questões de segurança, auditoria e conformidade.

As principais instalações de mainframe possuem departamentos independentes para a monitoração da segurança, através das informações do SMF. Outras instalações já estão colocando a segurança do z/OS em grupos totalmente autônomos, que monitoram UNIX, Windows e outros sistemas operacionais.

A reestruturação do grupo de segurança de mainframe:

(a) permite eventos de mainframe serem monitorados "fora da caixa" em um repositório centralizado;
(b) apresenta novas tecnologias e experiência para especialistas em segurança de mainframe, desejando expandir suas carreiras;
(c) permite que técnicos de segurança que não sejam de mainframe interajam ao que está acontecendo "dentro da caixa", o que torna uma proposta ganha/ganha para toda a organização.

3. O CUSTO DA VIOLAÇÃO DE SEGURANÇA DOS DADOS

De acordo com um estudo de 2015 da organização de pesquisa Ponemon Institute, patrocinado pelo International Business Machines Corp. o custo de uma violação de dados aumentou 23% desde 2013. O custo médio total de uma violação de dados era de US$ 3,8 milhões, e continua crescendo.

O estudo também relata que o custo incorrido para cada registro perdido ou roubado, contendo informações sensíveis e confidenciais aumentaram 6% em relação à média consolidada de $ 145 a $ 154.

Os números médios não definem uma imagem completa. Se olharmos para uma grande perda de varejo, você observará um impacto significativo.

A Target disse que as despesas brutas com a violação de dados foram de US$ 252 milhões. Se você subtrair o reembolso de seguro, as perdas caem para US$ 162 milhões. Deduções fiscais diminuem a receita líquida das perdas em US$ 105 milhões, o que ainda é uma perda significativa!

Target's losses attributed to data breach				
	Gross expenses	Insurance reimbursement	Pre-tax net expenses	Net of tax expenses
2013	$191m	$46m	$145m	$94m
2014	$61m	$44m	$17m	$11m
Total	**$252m**	**$90m**	**$162m**	**$105m**

Além das implicações financeiras, um compromisso dessa natureza também incluiria danos à reputação corporativa, perda de clientes e maior análise regulatória, além do dano pessoal aos gestores da empresa.

3.1 RESPONSABILIDADE PESSOAL

As violações de segurança sobre as informações podem ir além dos limites corporativos e expor empresas a ações legais indesejadas. Exposições de segurança derivadas do roubo de dados levou a três ações judiciais contra o Secretário de Assuntos dos Veteranos dos Estados Unidos. O roubo foi o resultado da transferência de dados para um laptop que foi posteriormente roubado de um endereço privado. A violação afetou 26,5 milhões de registros, com um estimativa entre US$ 100 milhões e US$ 500 milhões para prevenir e cobrir possíveis perdas pelo roubo de dados.

3.2 OS REGULADORES COMETH

Se já é muito ruim ter dados violados, incluindo o envolvimento do próprio responsável pela segurança, e ainda ter clientes não muito contentes com episódios de violação, a verdadeira dor está prestes a começar quando a sua empresa atua num setor da indústria regulamentado, já que as violações de segurança refletem muito mal nessas condições.

Haverá maior pressão para novas regulamentações e mais controle. Tudo será verificado num maior grau de detalhes nos próximos anos. Fornecer dados para os reguladores, responder a solicitações e corrigir questões, mesmo as menores, são extremamente demoradas e caras.

4. A EXPOSIÇÃO DE SEGURANÇA REAL AO DB2 NO Z/OS

O maior desafio de ataque a dados do DB2 no mainframe é obter as configurações com privilégio de Administrador do Sistema DB2. Comprometer e escalar os privilégios do DB2 a um usuário comum permite que o ataque aos dados do DB2 ocorra praticamente despercebido. Embora esteja se tornando mais difícil fazer isso atualmente no DB2, deve-se enfatizar o monitoramento de acessos a informações críticas, independentemente de um indivíduo ter ou não os privilégios adequados. Nem sempre é seguro supor que um produto de segurança do mainframe lhe proteja sempre.

Um bom exemplo disso ocorreu durante o desempenho de vulnerabilidade de rede em uma grande agência governamental. A rede foi comprometida (com autoridade da agência) e uma estação de trabalho foi invadida. Os arquivos de aplicativos relacionados a um processo em execução numa estação de trabalho foi examinado.
Agora, imagine um ID de logon e senha DB2 não criptografados sendo capturadas e utilizados para fazer login no Aplicativo DB2 do mainframe, com privilégios SYSADMIN. Esse cenário, num ambiente real, levariam a danos ilimitados.

5. FRAQUEZAS NO CÓDIGO DO DB2

Há 2 preocupações principais em relação ao código do DB2 desenvolvido e em execução nos mainframes:

1) Verificações aleatórias do código do DB2, usando o Web Services do mainframe, parecem estar alinhadas com as diretrizes e padrões de segurança atuais, mas "você não sabe o que não sabe". Revisões de aplicações no mainframe são quase inexistentes.

2) Muitas das aplicações legadas do DB2 foram escritas previamente aos impactos do 11 de setembro, quando não era justificado, em termos de custos, alterá-los para se ajustarem à consciência de segurança atual. A incapacidade de adaptar essas aplicações às atuais condutas de conscientização de segurança representa um grande problema para muitas empresas grandes e agências governamentais em todo o mundo. Especialmente, quando se considera que o data warehouse do DB2, que contém o principal ativo corporativo 'dados', é atualizado, verificado e acessado continuamente, suportando transações comerciais críticas. Lá residem os arquivos do cliente, informações médicas, registros de cartão de crédito, dados da previdência social, registros financeiros, e etc, todos os principais alvos de violações da segurança e informações ilegais. O governo respondeu com regulamentos severos como HIPAA, SOX e Graham Leach, além de multas financeiras às corporações que as deixaram de cumprir. Sob essas pressões, já era hora das empresas aderirem a metodologias de segurança que protegem o DB2 no z/OS para um nível maior.

6. UTILIZANDO REGISTROS SMF DO DB2 NO RASTREAMENTO DE EVENTOS

Existem mais de 100 tipos diferentes de registros SMF reservados pelo sistema operacional z/OS para várias funções operacionais. Números de registro acima de um determinado nível podem ser usados para produtos de fornecedores e programas de aplicativos de mainframe. O número de registro SMF oitenta (registro tipo 80) é usado por dois dos produtos de segurança de mainframe, comumente encontrados no mainframe. Um terceiro produto de segurança utiliza um número SMF atribuído a ele na instalação do produto (normalmente nº 231), enquanto a auditoria do DB2 usa registro SMF tipo 102.
Os registros SMF são gravados em arquivos, após o sistema operacional do mainframe realizar um evento.
O programador de sistemas de mainframe é responsável por definir o tamanho dos arquivos SMF primário e secundário. Quando o arquivo primário é preenchido, o secundário torna-se o principal e o arquivo SMF original é arquivado.

É normal em todas as empresas, que milhares de registros SMF sejam gravados diariamente. Esses registros mudam com frequência, tal como uma vez por dia, duas vezes por dia e até a cada hora, dependendo do volume de processamento de transações do cliente. O volume de registros SMF criado causam grandes dificuldades, impossibilitando o monitoramento do alto volume, por exemplo, de uma estação de trabalho em tempo real.
Outro problema apresentado é que esses registros SMF são normalmente disponibilizados com intervalos de tempo entre os relatórios. Então, se os relatórios nos registros SMF do DB2 de uma instituição financeira são utilizados para protegê-la de uma violação contra informações do cartão de crédito, elas só estarão disponíveis, na melhor das hipóteses, em incrementos a cada hora, o que possibilita uma janela de oportunidade para violação.

Outro problema em relação aos relatórios em lote nos registros SMF é que esses históricos bases para segurança, auditoria e relatórios de conformidade não são baratos. De fato, o custo da revisão manual de logs é muito alto.
Criação de logs com um objetivo de fornecer segurança é uma coisa, mas, na verdade, revisá-los e imprimi-los manualmente torna o processo muito caro.

Muitas vezes, as empresas parecem relutantes em gastar grandes somas na revisão desses logs. Mas se uma empresa não revisar um log, qual seria o objetivo de colocar esforços para armazená-los?

7. IMPLEMENTANDO REGISTROS DE AUDITORIA DO SMF NO DB2

A análise de log SMF é muito importante quando se trata de monitorar a segurança, auditoria do DB2 e conformidade. Uma das melhores maneiras de fazer isso é usando o recurso de rastreamento de auditoria do DB2. Este recurso deve estar ativado para cada tabela que se deseja monitorar. Isso é feito usando a cláusula AUDIT no momento de CREATE da tabela.

Além disso, as classes de rastreamento de auditoria devem ser ativadas para coletar os dados nos registros SMF do DB2. Cada Classe está associada ao tipo de eventos do DB2 que se deseja monitorar.

As Classes de Rastreio de Auditoria do DB2 são as seguintes:

Classe Um
Tentativas de acesso negadas pelo DB2 devido a autorização inadequada.

Classe Dois
Instruções explícitas GRANT e REVOKE e seus resultados. Esta classe não rastreia concessões implícitas e revogadas.

Classe Três
Instruções CREATE, ALTER e DROP que afetam as tabelas auditadas e os resultados dessas declarações.

Classe Quatro
Alterações nas tabelas auditadas.

Classe Cinco
Todos os acessos de leitura a tabelas que são identificadas com a cláusula AUDIT ALL.

Classe Seis
A ligação de instruções SQL estáticas e dinâmicas dos seguintes tipos:

Instruções INSERT, UPDATE, DELETE, CREATE VIEW e LOCK TABLE
para tabelas auditadas. Instruções SELECT em tabelas que são identificadas com a Cláusula AUDIT ALL.

Classe Sete
Atribuição ou alteração de um ID de autorização pelos seguintes motivos:

- Alterações através de uma rotina de saída (padrão ou escrita pelo usuário)
- Alterações através de uma instrução SET CURRENT SQLID
- Uma conversão de ID de autorização de saída ou entrada
- Um ID que está sendo mapeado para um ID RACF a partir de um tíquete de segurança Kerberos

Classe Oito
O início de um job utilitário e o final de cada fase deste.

Classe Nove
Vários tipos de registros gravados no IFCID 0146 pela função IFI WRITE.

Classe dez
(DB2 V9.1) CREATE e ALTER TRUSTED CONTEXT, estabelece informações de conexão confiáveis e alterna as informações do usuário.

Aqui está uma lista parcial dos eventos relacionados à segurança do DB2, comumente monitorados:

- Direitos de acesso
- Alterações de privilégios, alterações explícitas de privilégios, bem como alterações administrativas Atividade SYSCTRL e SYSADM
- Alterações na autorização
- Queda de tabelas
- Inserir / alterar registros
- Acessando dados de IDs não autorizados
- Instruções GRANT / REVOKE

Para algumas classes, outras atividades nas informações da trilha de auditoria do DB2, importantes razões forenses e resposta a incidentes, é a instrução SQL real que estava sendo realizada no momento do incidente. É uma impressão digital para a tabela, linha e coluna que o usuário estava procurando no momento. Infelizmente, está localizado atrás de um complexo índice de configurações de bits no registro da trilha de auditoria do SMF do DB2 e de difícil interpretação.

O recurso DB2 Audit Trace é historicamente conhecido por incluir sobrecarga adicional da CPU.

O DB2 melhorou progressivamente ao usar esse recurso a cada novo release, trazendo uma redução drástica nessa sobrecarga. As estatísticas mais recentes da IBM indicam que introduzirá menos de 10% de sobrecarga adicional da CPU, por transação, se todas as classes estiverem ativadas.

8. PENSANDO "FORA DA CAIXA"

A plataforma do sistema operacional de mainframe é a principal dispositivo de processamento de transações e sempre sustentou a tecnologia de segurança líder do setor. Durante muitos anos de serviço, geralmente sob condições mais exigentes que se possa imaginar, ele sobreviveu. Provou-se mais de uma vez ser fundamental, e foi premiado com o mais alto certificação de segurança comercial. No entanto, em um mundo em mudanças, com um aumento de segredos comerciais perdidos, roubo de identidade pessoal e irregularidades de funcionários, associados e contratados, os mecanismos de segurança mais fortes são essenciais. O conceito de segurança do mainframe de "permitir" ou "negar", simplesmente não podia ser suficiente. Era necessário mais salvaguardas que ajudassem a proteger usuários e dados com recursos que não eram possíveis até então.

A resposta para levar a segurança do mainframe para o próximo nível é; integrando a segurança de mainframe "sim" ou "não" com produtos de segurança de rede já existentes. Os profissionais de segurança do mainframe precisavam de ferramentas para realizar esse feito em um mundo onde era essencial o lema "Confie, mas verifique". Há uma variedade de Gerenciamento de Log e produtos SIEM que suportam o DB2 e que já podem ser implementados em suas próprias organizações.
Esses produtos ficam fora do mainframe, na rede, e coletam o log de eventos de firewalls, UNIX, Windows e outros sistemas operacionais. Contudo, ainda não é tão frequente que administradores de Segurança no mainframe se utilizem desses recursos.

8.1 GERENCIAMENTO DE LOGS

Os produtos de gerenciamento de log estão disponíveis em fornecedores comerciais, incluindo IBM e outros. Eles são projetados para coletar dados brutos do log. Uma solução parcial no mainframe é rotear os logs do console diretamente para o software de Gerenciamento de Log. Esta é apenas uma solução parcial porque o console registra os dados sozinho e não contêm todas as informações necessárias para monitorar completamente o ambiente mainframe. Uma melhor abordagem para o Gerenciamento de Log é usar a combinação de dados brutos, de logs do console, arquivos de log de segurança e dados SMF. Os problemas surgem quando você tenta enviar as informações combinadas ao software Log Management, porque o volume dos dados que viajam pela rede cria um tempo de espera. A informação não chega de maneira oportuna, conforme exigido pelos mandatos regulamentares.

8.2 PRODUTOS SIEM COM SUPORTE AO DB2

Os produtos SIEM coletam eventos de segurança de várias fontes além do mainframe.
Espera-se que os eventos sejam compactados pelo software Agente executado em um dispositivo remoto. Os registros SMF do DB2 podem apresentar um tamanho excessivo (o SQL pode ter apenas 4k) e deve ser filtrado ou compactado para qualquer produto SIEM. O processo de leitura dos logs de segurança e a compactação em avisos e alertas ocorre por um processo de Agente remoto, que reside no mainframe. Isso poupa custos e tráfego de rede relacionados no armazenamento de dados em excesso no repositório central. Fornecedores de produtos SIEM, como a IBM, geralmente oferecem processos em batch e em tempo real para coletar informações do DB2 no mainframe.

Uma maneira de aproveitar o investimento já realizado é capitalizar a ação é pensar ‘Fora da Caixa’, integrando eventos de mainframe em um dos produtos que sua empresa já investiu.

8.3 SOLUÇÕES PRÓPRIAS DE MAINFRAME PARA O DB2

O desenvolvimento de uma aplicação Agente para ler e monitorar os registros SMF do DB2, registros SMF não DB2, mensagens de console, mensagens de aplicativos e produtos de fornecedores é uma tarefa extremamente trabalhosa. Os registros SMF do DB2 são considerados um dos formatos de registro mais complexos e só pode ser interrompido por um experiente desenvolvedor de sistemas. Não incluir os registros SMF do DB2 em uma solução desenvolvida internamente pela sua equipe de desenvolvedores seria como produzir algo que gerasse um resultado altamente ineficaz.

Outro ponto interessante é que na Lei Sarbanes-Oxley de 2002, a definição de Separação de Deveres especifica que o pessoal de segurança que administra ou monitora não deverá escrever códigos de segurança. Em essência, códigos desenvolvidos internamente, incluindo monitores de log e saídas escritas pela própria equipe de segurança da organização, viola a própria auditoria.

Dito isso; caso ainda assim sua equipe decida prosseguir, existem algumas técnicas complicadas e problemas de design que precisam ser resolvidos antes mesmo de começar. Esses problemas incluem:
• Tempo assíncrono
• Consumo inaceitável de CPU e recursos de rede
• Conversão de dados binário para texto
• Entregar as informações em tempo hábil, para que possam ser tomadas ações imediatamente em cima de cada evento.

A complexidade e os custos relacionados ao desenvolvimento de um aplicativo 'caseiro', geralmente são deixados de lado pela gerência quando comparado ao custo de compra de software de fornecedores confiáveis e que já atuam no mercado.

9. SUMÁRIO:

O DB2 do z/OS chegou para ficar e crescerá apenas para acomodar os requisitos de armazenamento de dados e transações comerciais corporativas. No passado, a ênfase na segurança sempre parecia estar em sistemas distribuídos. No entanto, os novos regulamentos governamentais nivelaram o campo para incluir todos os dados, conforme o FISMA (Federal Information Security Management Act) de 2008. Todo computador e rede do governo é essencialmente necessário para proteger seus dados confidenciais e quaisquer outros tipos de registros.
Esses padrões estão se disseminando comercialmente com a fusão de entidades governamentais e comerciais. O SOX e HIPAA não têm limites em relação ao comprometimento de dados críticos.

Neste artigo, abordamos algumas questões importantes relacionadas a violações de segurança, incluindo como a plataforma de mainframe funciona na monitoração dos registros, quais armadilhas estão nos métodos tradicionais de uso de registros SMF do DB2 para rastreamento de eventos, e como a plataforma de mainframe pode ser modernizada para fornecer monitoramento de segurança aprimorada nos registros importantes e confidenciais. Um ataque, especialmente no z/OS do DB2 para hackear os privilégios das configurações do Administrador do Sistema DB2, é uma falha de segurança. Portanto, não é mais eficiente ou seguro confiar apenas nos sistemas de segurança e relatórios batch que funcionam estritamente dentro do mainframe, ou nos registros de incidentes onde a segurança foi violada. Agora é possível usar produtos para monitorar o mainframe de fora para dentro.

Entre os vários tipos de produtos de segurança que podem funcionar fora do mainframe estão o Gerenciamento de Log, o SIEM (Sistema de Gerenciamento de Eventos de Segurança) e produtos que suportam o DB2. Cada um desses produtos tem seus Prós e Contras e não há nenhuma solução que sirva para todos os casos. O ponto importante é que todas essas soluções são mais econômicas, eficientes e mais rápidas que os modelos anteriores, no combate a novos tipos de ameaças à segurança.

Então, como escolher o software correto entre as muitas alternativas? Enquanto se escolhe um produto de segurança específico capaz de funcionar fora da plataforma mainframe, certos fatores precisam ser verificados. Aqui estão alguns critérios que você pode considerar ao avaliar um produto de segurança para sua empresa:

- Ser escalável
- Fácil de usar
- Espaço para crescimento lateral
- Monitoramento de eventos em tempo real 24/7
- Facilidade de configuração e instalação
- Pequena carga de processamento e baixo impacto no desempenho sobre sistemas de mainframe

Embora o custo de proteção eficaz dos dados seja alto, o custo de uma violação de segurança é ainda maior, considerando as novas leis que regem a proteção dos dados. As empresas podem dar um suspiro de alívio agora que existem softwares de mainframe econômicos e abrangentes no mercado.

Esses produtos atendem às necessidades atuais das empresas na área de registros de segurança confidenciais de seus próprios negócios, assim como as de seus clientes, e possuem todas as qualidades necessárias para combater as ameaças à segurança. Eles trabalham eficientemente com produtos de segurança de mainframe já existentes e fazem uso do SMF e console de mensagens de formas apropriadas. Eles são capazes de rastrear os eventos auditados do DB2 e várias ameaças internas, fornecendo alertas de mainframe em tempo real e integrando-se facilmente a outros monitores de segurança.

Empresas proativas, com um histórico de monitoramento de logs de segurança externa, estão na vanguarda dos requisitos governamentais e possuem uma estrutura sólida para gerenciar dados do DB2 e seus riscos associados. Isso os coloca, independentemente do seu negócio, em uma melhor posição competitiva, com uma postura de segurança ideal que permita participarem da evolução do compartilhamento de dados.

SOBRE OS AUTORES:

Jerry Harding
Jerry Harding é CEO da Type80 Security Software, Inc. Ele tem mais de 25 anos de experiência em programação de sistemas de mainframe, fornecendo serviços profissionais para clientes comerciais e agências governamentais. Ele também tem mais de 15 anos de segurança experiência, incluindo o treinamento da Agência de Contra Inteligência da OTAN (ACE) CI), a Sede Suprema da Allied Powers Europe (SHAPE), bem como outros e organizações privadas.

Stephen D. Rubin
Stephen D. Rubin é o fundador e presidente da MMI. Sob sua liderança, o MMI tem um histórico de 20 anos de sucesso financeiro na criação de mercados de negócios para informações serviços de tecnologia (TI) na América do Norte. As áreas de negócios incluem treinamento, serviços de consultoria e software. A MMI treinou mais de 3.000 estudantes de TI representando mais de 400 empresas em design de banco de dados, segurança da informação, planejamento de capacidade e desenvolvimento de aplicativos distribuídos. Os compromissos de serviço profissional incluíram segurança da informação, consolidação de servidores e auditoria do planejamento de capacidade e metodologias de estorno para os setores público e privado. .

William Buriak
William Buriak tem mais de 25 anos de experiência em tecnologia da informação com um extensa experiência em serviços financeiros, assistência médica e assistência técnica e de gestão consultando. Bill é um executivo sênior com experiência comprovada em planejamento, desenvolvimento e implementação de soluções inovadoras e econômicas para lidar com problemas de negócios. Ele possui ampla experiência reconhecida no gerenciamento de sistemas mainframe, baseados na Web e sistemas distribuídos. Possui extensas qualificações, incluindo habilidades de gerenciamento de fornecedores, construção de consenso e planejamento estratégico. Atualmente trabalhando na área de Engenharia de Segurança de um grande banco mundial, o Sr. Buriak é responsável por conformidade e controle de um grande número de produtos globais.

SOBRE A SDS

A Software Diversified Services (SDS) foi fundada em 1982, suporta mais de 20 produtos para sistemas mainframe z/OS, MVS, VSE e VM para mais de 1.000 clientes em todo o mundo, bem como soluções de criptografia para Windows, UNIX, Linux e AIX.
Dentre os clientes incluem muitas empresas globais no setor bancário, financeiro, de seguros e de varejo, além de locais, governos estaduais e nacionais.
Segurança, criptografia e gerenciamento de rede são os focos atuais, além do monitoramento de desempenho, relatório e aplicativos de distribuição e cliente-servidor.
No SDS, o suporte técnico trabalha em conjunto com o desenvolvimento. O SDS é conhecido por ter a mais alta qualidade em software, documentação e suporte técnico no negócio. O suporte técnico da SDS foi classificado como número 1 pelo prestigiado Boletim IBEX.

SDS
1322 81st-Ave NE
Minneapolis, MN 55432-2116
Telefone: 763-571-9000
info@sdsusa.com
www.sdsusa.com