Sumário

1. OBJETIVO

Fornecer orientações gerais para configurações de log's e de auditorias de servidores e sistemas dentro da CPFL. É fundamental que os administradores de sistemas e o departamento de segurança usem as diretrizes especificadas para assegurar a configuração adequada e necessária na coleta de dados de log´s. O cumprimento destas diretrizes ajudará a garantir a segurança de sistemas e servidores, e de todos os recursos que se destinam a proteger.
Os riscos de acessos não autorizados e indevidos para sistemas e informações da DXC e de seus clientes podem ser reduzidos através de auditorias de acesso aos sistemas e informações. O registro de log's, acompanhamento periódico e, a auditoria aos servidores permitem a descoberta precoce e a investigação de ações suspeitas antes de consequências adicionais ocorrerem. A fim de detectar as ameaças relacionadas com o acesso não autorizado e indevido, a auditoria deve envolver a análise e a verificação de ativos críticos de uma organização. Além disso, a auditoria deverá examinar e verificar a integridade, bem como a legitimidade dos acessos registrados, podendo ser tanto contínua como por amostragem, sendo que no segundo cenário, a amostragem de todas as operações, acrescenta imprevisibilidade suficiente para o processo de detectar ou impedir uma pessoa de lançar um ataque contra sistemas.

2. ÂMBITO DE APLICAÇÃO

2.1. Empresa

Estas diretrizes se aplicam a todos os administradores de sistemas e integrantes dos times responsáveis pela manutenção, administração e / ou de auditoria e sistemas de servidores que são escopo do contrato de infraestrutura de TI.

2.2. Área

Esta orientação deverá ser aplicável aos servidores e sistemas que a DXC gerencia para a CPFL e que possuem política de auditoria de registro de log's.

3. DEFINIÇÕES

TI - Tecnologia da Informação

DoS – Negação de Serviço

NTP – Protocolo de Tempo de Rede

S.O – Sistema Operacional

4. DOCUMENTOS DE REFERÊNCIA

Não aplicável.

5. RESPONSABILIDADES

DXC Technology.

6. REGRAS BÁSICAS

6.1. Riscos de Segurança

Através da adoção de boas práticas de segurança do sistema, a DXC pode melhor assegurar a confidencialidade, integridade e disponibilidade das informações. Alguns dos riscos e ataques mais comuns que os servidores e sistemas são suscetíveis:

- Ataque de força bruta, Acesso não autorizado, Violação de dados, Ataques do tipo DoS, Port Scanning Attack

6.2. Armazenamento de log´s

Armazenamento de log´s, acompanhamento periódico e auditoria de servidores oferecem a oportunidade de investigar e descobrir ações suspeitas antes de ocorrerem.

Devido à natureza do negócio, qualquer comprometimento com a confidencialidade, integridade ou disponibilidade das informações da rede de uma empresa pode prejudicar a capacidade para realizar negócios. A exposição pública adversa provocada pelo vazamento ou o acesso não autorizado não só prejudica a credibilidade dentro do mercado mas, também, impactam os contratos existentes, colocando em risco a saúde financeira da DXC e de seus clientes.

Os requisitos mínimos cobrem aspectos críticos essenciais para proteção dos dados e apoiam a detecção precoce e a investigação de ações suspeitas antes dos problemas ocorrerem.

Os itens a seguir descrevem os requisitos relacionados a sistema operacional, política e registro de log´s de administração em servidores e sistemas:

1. Assegurar que todos os servidores ou sistemas possuem armazenamento de log´s habilitado;

2. Registrar todas as mensagens do sistema operacional incluindo, mas não limitados a:

- Login
- System Health
- Alterações de configuração
- Informações sobre inicialização

3. Registrar todos os acessos administrativos ao servidor ou sistema. Esse acesso deve incluir:

- Identidade do administrador ou usuário
- Data e hora de logon e logoff.
- Atividades realizadas

4. Sempre que possível, os log´s devem ser armazenados em um sistema centralizado para proteger sua integridade e para fornecer uma análise de dados offline e geração de relatórios. Isso também pode fornecer um método mais robusto para a análise de vários log´s de sistemas e apresentar um relatório agregado das atividades de rede / sistemas.

5. Os log´s devem ser mantidos por um mínimo de 90 dias.

6. Todos os dispositivos de armazenamento e servidores devem ser configurados para sincronizar seus horários com um servidor NTP. Isso fornecerá informações de tempo precisas sobre os logs para solução de problemas e necessidades de investigação forense.

6.3. Auditoria / Monitoração

Os itens a seguir descrevem os requisitos mínimos relacionados a auditoria e monitoramento de servidores e sistemas:

- Sempre que possível, um analisador de log robusto e uma ferramenta de relatórios deve ser utilizado para auxiliar no monitoramento / auditoria.

Log´s devem ser analisadas conforme detalhado abaixo. A intenção é garantir que o servidor e / ou sistema está funcionando de maneira estável, a política aplicada está funcionando adequadamente para proteger os recursos de dados, e qualquer tentativa de burlar o sistema ou a sua política serão identificadas. As análises de log a seguir devem ser realizadas:

Diária - monitorar os registros que abrangem um período de 24 horas. Isto irá fornecer uma visibilidade rápida das atividades do dia passado incluindo acesso ao servidor/sistema, modificações de políticas/regras e qualquer risco potencial quando aplicável, e riscos imediatos na rede. Servidores ou sistemas de menor criticidade devem ser revistos por amostragem, de forma que cada log do sistema seja revisto pelo menos uma vez por semana.

Semanal - Análise dos dados da semana anterior, rastrear qualquer alteração e desenvolver uma lista de possíveis anomalias nos servidores / sistemas / política que possa apontar para um problema de violação da segurança ou de sistema.

Mensal - Garantir que as políticas dos servidores estão em conformidade com a Política de Segurança da DXC/CPFL e que o conjunto de regras esteja configurado de modo que o servidor ou o sistema as executem com a máxima eficiência.

- Devem ser fornecidos acessos "adequados" para as pessoas indicadas nos times, a fim de facilitar a análise e investigação de apoio dos logs de auditoria.

Se depois que um administrador de sistema analisou uma log de sistema e uma falha de segurança é suspeita, deve ser comunicada ao grupo responsável pela análise de Incidentes de Segurança. Idealmente, o administrador do sistema não deve tomar medidas para parar a atividade a menos que explicitamente indicado pela equipe de serviços de segurança. O principal objetivo é rastrear o(s) responsável(eis) pela violação. Se as violações forem interrompidas demasiadamente cedo, a vulnerabilidade relativa à exposição e/ou a identidade dos atacantes pode ser perdida. Entretanto, os

fatores mais importantes a serem considerados devem ser a segurança, a prevenção de novos incidentes e o aumento da exposição da DXC e/ou o cliente.

Para executar a medição e aderência automática do processo na Operação, se faz necessário uma ferramenta que será disponibilizada pela CPFL. Após a aquisição, o processo deverá ser revisado e se preciso, será adaptado. Enquanto isso o processo será medido de forma manual.

6.4. Processos Paliativos

Como não existe uma ferramenta de monitoração de LOGs, foram desenvolvidas soluções que atendam às necessidades conforme segue abaixo o descritivo:

UNIX

Referente a auditoria, o que é executado no servidor:

- Implementada uma configuração onde todos os comandos executados no Sistema Operacional ficam registrados com timestamp, abaixo seguem as características desse log: Caminho = /var/adm/hist

- Nome do arquivo = o arquivo é definido através do nome do usuário, ip ou nome da estação de onde o usuário inicia a conexão e data do início da conexão.

- Conteúdo = Todos os comandos executados no Sistema Operacional ficam registrados com timestamp nesse arquivo.

- Nesse log não é efetuado verificação diária, a análise é realizada apenas quando ocorre algum incidente.

Ambiente Distribuído (Windows / Vmware / Citrix / E-mail / Middleware)

Referente a auditoria, o que é executado no servidor:

- Os logs de eventos do S.O são sistematicamente coletados várias vezes ao dia (Sistema, Segurança e Aplicação), e consolidados em um servidor com estrutura de diretórios, separadas por cada host. A retenção é realizada conforme a política da CPFL além disso, é realizado backup diário dos servidores, portanto, é possível obter um log do próprio servidor caso necessário e conforme política de backup vigente.

- Atualmente não temos nenhuma aplicação que faça a análise e correlação destes eventos, cabendo ao time de suporte a análise individual dos mesmos quando necessário.

- Nos controladores de domínio, é utilizada a ferramenta Manage Engine ADAuditPlus.

- Periodicamente são realizadas análises de Conformidade Regulatória no ambiente (Security Reviews), de acordo com documentos e procedimentos estabelecidos nos Apêndices Técnicos da Política de Segurança.

BACKUP

- Os ambientes Netbackup são responsáveis pelo backup do ambiente, o armazenamento dos logs é realizado de 3 diferentes maneiras, sendo:

Activity Monitor = Nesta sessão existem todos os logs de execução do ambiente por 72 horas, onde podem ser reprocessados, analisados e validados.

Status Report = Nesta sessão temos o relatório por categorias e filtros, onde são armazenados 28 dias de todas as execuções. O filtro pode ser realizado por política, cliente, retenção e períodos.

Catalog = No catálogo, todos os backups executados podem ser consultados a qualquer momento e ficarão retidos pelo tempo do armazenamento do backup. O filtro pode ser realizado por política, cliente e período de armazenamento.

SAP

- Os ambientes SAP estão configurados para coleta de logs internamente via SM19, seguindo a Política de Segurança atual.

- Os logs são retidos por 90 dias. (Garantidos pelo Backup) e são analisados somente em caso de incidentes.

Oracle

- Os ambientes Oracle estão configurados para coleta de logs internamente via parâmetro de auditoria interna do banco de dados (audit_trail=DB), seguindo a Política de Seguranca atual. (Somente LOGs de Audit).

- Os logs são analisados somente em caso de incidentes, em caso de Alertas do Oracle (log técnico crítico) ou devido a solicitações da equipe de auditoria.

SQL Server

- O Audit Log é habilitado apenas nos ambientes SOX, auditando exclusivamente os acessos dos DBA's.
- As instancias possuem apenas as logs de evento do sistema.

Redes

- Hoje existe um servidor de LOG (syslog), onde todos os log´s referentes aos equipamentos de rede, são por 90 dias.

GIS

- Como os Ambientes GISD possuem diversas plataformas (Windows, AIX, Oracle e SQL), as monitorações ou ferramentas, são das próprias equipes, caso existam.

7. CONTROLE DE REGISTROS

Identificação	Armazenamento e Preservação	Proteção (acesso)	Recuperação e uso	Retenção	Disposição
Incidente	CRM Dynamics	Backup	Demanda	Backup	Deletar

8. ANEXOS

Não aplicável

9. REGISTRO DE ALTERAÇÕES

9.1. Colaboradores

Empresa	Área	Nome
DXC	SSIO	Denis Bernardo Petrasse
DXC	SSIO	Daniela Aparecida Saran
DXC	SSIO	André Sanches
DXC	SSIO	Hidebrando Aires Matias
CPFL	Governança	Heliane Pontes

9.2. Alterações

Versão Anterior	Data da Versão Anterior	Alterações em relação à Versão Anterior
X	24/11/2010	Criação do documento
X	15/07/2011	Revisão geral do documento
X	21/02/2013	Revisão geral do documento
1.0	06/08/2014	Revisão geral do documento
1.1	03/03/2016	Revisão geral do documento - Padrão CPFL e publicação no GED
1.2	07/03/2016	Correção do índice
1.3	21/02/2018	Revisão geral do documento
1.4	02/03/2018	Revisão geral do documento e adequação ao modelo para elaboração de documentos no GED