INSTITUTO FEDERAL
Rondônia

INSUFFICIENT LOGGING & MONITORING

Por que a falha em verificar os logs é tão perigosa quanto o ataque em si.

Leyukezer C. Lima

TÓPICOS

1. O que são os logs e o monitoramento de logs?
2. O que é Insufficient Logging & Monitoring?
3. O Caso Equifax (2017)
4. A Origem do Problema

INSTITUTO FEDERAL
Rondônia

O QUE SÃO OS LOGS E O MONITORAMENTO DE LOGS?

Logs são registros cronológicos de eventos gerados por sistemas, aplicações, dispositivos de rede ou qualquer componente de TI. Eles são o "diário de bordo" da sua infraestrutura digital.

Estrutura de um Log:

- Timestamp: Data e Hora exata do evento.
- Identificador/Nível: Severidade (Info, Warn, Error, Debug, Fatal).
- Origem: qual componente gerou o log (nome do servidor/aplicação).
- Mensagem: Descrição do evento em texto livre.
- Id do Usuário/Sessão: Quem estava envolvido na ação.
- Endereço Ip: De onde a requisição se originou.
- Método e Endpoint: endereçamento da ação (POST /api/v1/login).

```json
{
  "timestamp": "2024-01-15T10:30:00Z",
  "level": "ERROR",
  "userId": "user123",
  "sessionId": "sess_abc789",
  "ipAddress": "192.168.1.100",
  "event": "Failed login attempt",
  "details": "5 consecutive failures from same IP"
}
```

O QUE SÃO OS LOGS E O MONITORAMENTO DE LOGS?

Exemplo de Log

```text
[2023-10-27 14:35:12] [WARN] [Auth-Service] [IP: 189.123.45.67] Tentativa de login falha para o usuário 'joao.silva'.
[2023-10-27 14:35:15] [ERROR] [Payment-Service] [UserID: 12345] Falha ao processar pagamento. Transação ID: TX-78910.
```

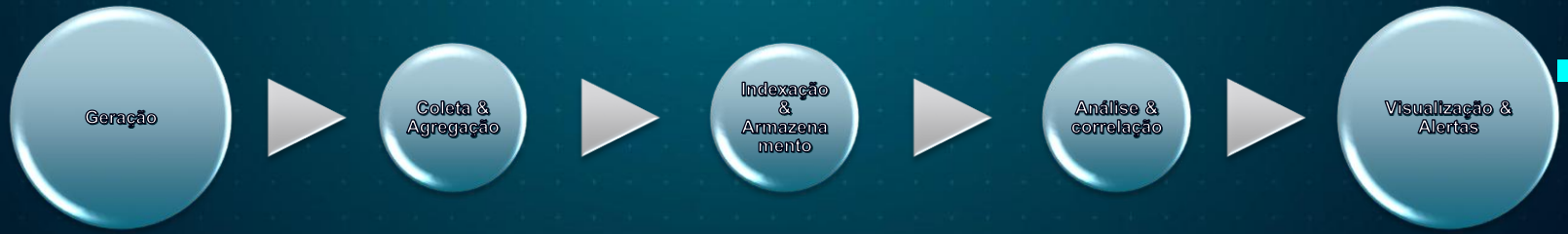
Copy Download

Objetivos dos Logs:

1. Debugging: Encontrar a causa raiz de erros e falhas.
2. Auditoria: Rastrear quem fez o quê e quando.
3. Análise de desempenho: Identificar gargalos e lentidão.

O QUE SÃO OS LOGS E O MONITORAMENTO DE LOGS?

Agora o Monitoramento de Logs é o processo ativo e contínuo de coletar, agregar, analisar e alertar sobre os dados contidos nos logs. Não basta apenas gerar logs; é preciso extrair significado deles em tempo hábil.



O QUE É INSUFFICIENT LOGGING & MONITORING?

É a falha de segurança que ocorre quando um sistema enfrenta os seguintes problemas.

- **Não Gera Logs suficientes.**
- **Gera logs mas não possuem detalhes úteis.**
- **Não Há monitoria proativa desses logs com possíveis atividades suspeitas.**
- **Não à alertas direcionados aos responsáveis quando ameaças são detectadas.**

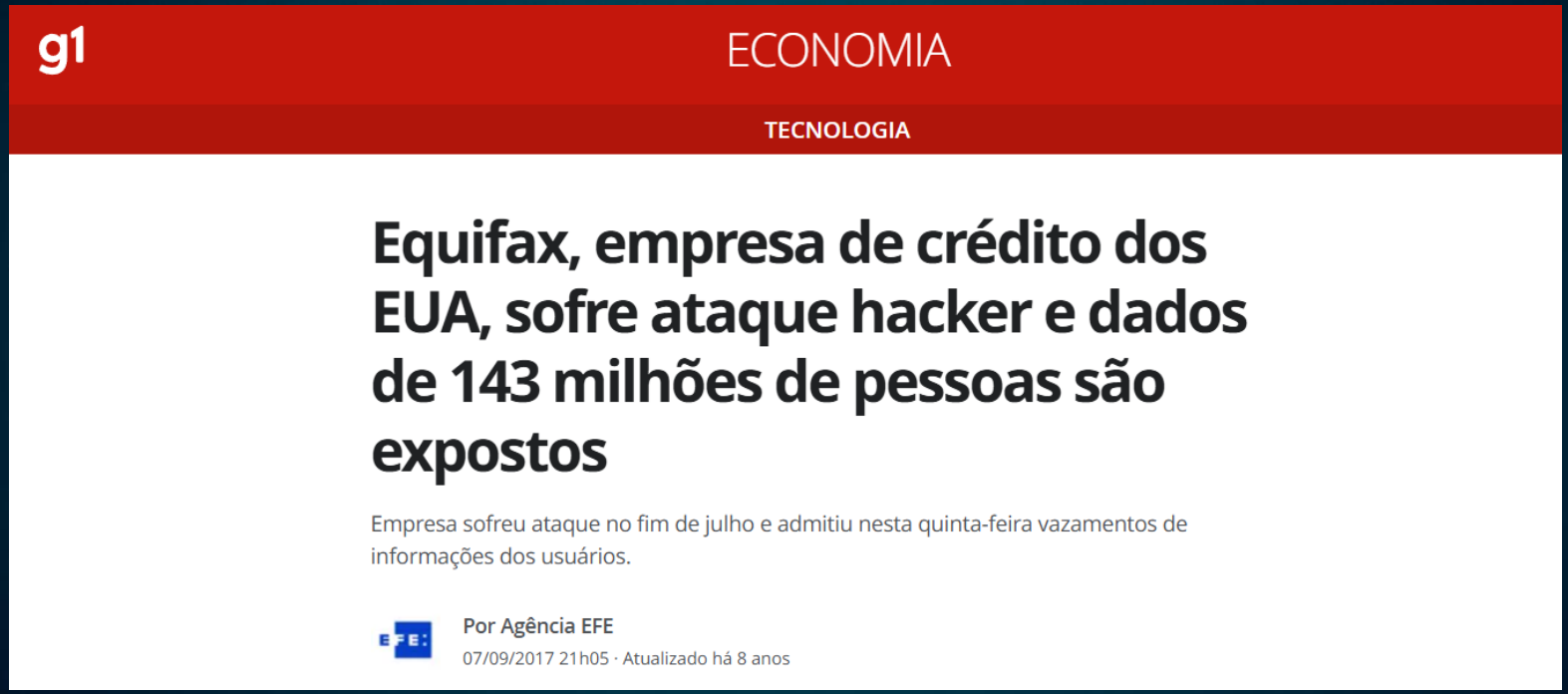
O QUE É INSUFFICIENT LOGGING & MONITORING?

É a falha de segurança que ocorre quando um sistema enfrenta os seguintes problemas.

Agentes/Vetores	Fraquezas de Segurança	Impactos
Específico da API: Explorabilidade	Prevalência: Detecção	Técnico: Específico do Negócio
Atacantes podem tirar proveito de pouco log e monitoramento para abusar de sistemas sem serem notados.	Sem log e monitoramento, ou log e monitoramento insuficiente, é quase impossível rastrear atividades suspeitas e dar respostas à elas tem tempo hábil.	Sem visibilidade do que está ocorrendo de atividades maliciosas, atacantes possuem tempo para comprometer completamente sistemas.

Tabela da OWASP API Security Top 10

O CASO EQUIFAX (2017)



g1

ECONOMIA

TECNOLOGIA

Equifax, empresa de crédito dos EUA, sofre ataque hacker e dados de 143 milhões de pessoas são expostos

Empresa sofreu ataque no fim de julho e admitiu nesta quinta-feira vazamentos de informações dos usuários.

Por Agência EFE

07/09/2017 21h05 · Atualizado há 8 anos

A ORIGEM DO PROBLEMA

Dentre todas as seguranças do sistema, um fator nada fora do comum mas que custou caro.
A especulação é de que os sistemas de segurança da Equifax **geraram logs** da atividade suspeita. No entanto, o certificado digital usado para criptografar e assinar os logs havia **expirado há 10 meses**.

Por causa disso, os sistemas de monitoramento **não conseguiram processar os logs** e, consequentemente, **nunca geraram um alerta**.
Os invasores tiveram acesso livre aos sistemas por **74 dias** antes de serem descobertos.

CHECKLIST DE BOAS PRÁTICAS

INSTITUTO FEDERAL
Rondônia

É a falha de segurança que ocorre quando um sistema enfrenta os seguintes problemas.

- **Gerar log de todos os eventos de login.**
- **Gerar logs de operações (crud).**
- **Checar integridade dos logs.**
- **Centralizar em um local seguro (de preferencia com mensalidade paga em dias).**
- **Alertas para atividades de alto risco.**
- **Testes regulares de alertas.**
- **Revisão periódica das regras.**
- **Plano de resposta a incidentes.**

Bons Estudos!

INSTITUTO FEDERAL
Rondônia