DESAFIO TÉCNICO ZE DELIVERY – CARLOS ADRIANO DE OLIVEIRA SILVA

Case Zé Connect

Como a aplicação Zé Connect que trabalhará em ambiente público (internet), proponho a seguinte estrutura:

- Criação do *cluster* com *LoadBalancer* entre os servidores que vão rodar a aplicação, para garantir que haja balanceamento e alta disponibilidade;
- Aplicar uma *baseline* de *hardening* de segurança do sistema operacional dos servidores que farão parte do cluster que executará a aplicação;
- Instalação de um EDR (*endpoint detection and response*) nos servidores do cluster da aplicação Zé Connect, oferecendo segurança ao sistema operacional executado no servidor;
- Implantação de um DBF (*database firewall*) no banco de dados da aplicação, visando garantir auditoria e supervisão das atividades executadas no banco de dados, bem como proteção contra ameaças de banco de dados como SQL Injection, em casos que o WAF não conseguir bloquear o ataque;
- Implantação de um IPS (*intrusion prevent system*) para analisar o trafego a ser direcionado a aplicação e tomar ações de bloqueios, essas de acordo com o tipo de assinaturas que o IPS prover;
- Implantação de uma solução WAF (*Web Aplication Firewall*) como front da aplicação, provendo segurança para que códigos maliciosos como SQL Injection, Cross Script Site, DDOS, quebra de autenticação e outros ataques não passem para aplicação;
- Solicitar a equipe SOC (*Security Operation Center*) a inclusão dos log's do WAF, DBF e EDR no SIEM, para monitorar e tratar os incidentes gerados. Nos casos de incidentes de maior severidade, encaminhar a equipe de resposta a incidentes;
- Implantação e configuração de uma solução de DLP (*Data Loss Prevention*) nos endpoints da empresa, visando evitar que dados sensíveis (previamente definidos no escopo de LGPD junto ao DPO) que sejam acessados, saiam da empresa de forma indevida ou não autorizada. O DLP também irá possibilitar analise e monitorar o uso dos dados pelos usuários;
- Caso não exista, criaria um processo de *vulnerability management* periódico para realizar scans de vulnerabilidade nos servidores utilizados pela aplicação, bem como a parte publica (aplicação web Zé Connect), dessa forma, mapeamos as vulnerabilidades encontradas e mitigamos para que não haja vulnerabilidades que possam ser exploradas e causarem danos;
- Criação ou uso de um processo de pentest periódico na aplicação web (Zé Connect), para verificar que as vulnerabilidades mapeadas e mitigadas com o processo de vulnerability management, foram efetivos. Caso seja possível realizar algum ataque, evidenciar o tipo de ataque e prover a mitigação. Após, executar novamente o pentest para validação da mitigação e verificado que não existe mais vulnerabilidades, realizar o pentest em intervalos periodicos;
- Criação de um processo para utilização de um sistema de análise de vulnerabilidades em códigos, como exemplo os sistemas SonarQube ou o Checkmarx. Nesse fluxo o desenvolvedor irá inserir o código feito na solução para ser analisada e após análise, a solução devolve com os possíveis problemas ou não, de segurança no código. O desenvolvedor volta a atuar no código executando as correções propostas para que o código não contenha vulnerabilidade e submete novamente a análise. O desenvolvedor só poderá subir com o código após validação de que o código está seguro e não possui vulnerabilidades;

- Criar um fluxo de acesso aos servidores da aplicação e banco de dados do Zé Connect, somente através de uma solução de PAM (*Privileged Access Management*) com cofre de senhas. Com tal solução, podemos monitorar com gravação de tela durante toda a sessão do acesso remoto bem como gravar o histórico comandos executados na sessão remota, possibilitando auditar o que é feito nos acessos remotos aos servidores e banco de dados. A solução também oferece gestão dos acessos e limitações do que pode ou não ser feito na sessão, bem como o tempo de duração da sessão;
- Após validar os passos acima, colocar um processo de autenticação no sistema, integrado a serviços de MFA (*multi-factor authentication*). Isso garantirá que o acesso só será feito por aquele usuário caso ele mesmo aprove o acesso através do MFA.

Educação de pessoas:

- Contando com a equipe de RH e marketing, proporia a criação e execução de campanhas de segurança da informação, através das vias como:
    - E-mail com: informativos, dicas e boas práticas de segurança em corporações, expondo quais os maiores problemas enfrentados hoje pelas empresas, quem é o maior causador dos problemas e formas de evitar que o problema ocorra. Além do e-mail, faria periodicamente techtalks abertos aos colaboradores para tratar de temas de segurança da informação, cybersegurança, LGPD e demais temas pertinentes. **OBS: Nesse caso, apesar de não gostar de recomendar empresa especifica, viabilizaria a contratação dos Hackers Rangers (https://hackerrangers.com/) empresa focada em promover cultura de segurança da informação em outras empresas. Utilizam de plataformas de gamification, troféus e brindes por conquistas, treinamentos digitais sobre códigos maliciosos, segurança em e-mail, LGPD e demais assuntos, pois o jeito de trabalho da empresa é inovador e nada maçante, o que garante maior absorção dos colaboradores nos treinamentos.**
- Especificamente para os desenvolvedores, chamaria um parceiro para trabalhar o tema e a cultura de devsecops, mostrando aos desenvolvedores que dá para executar o trabalho de forma bem-feita, ágil e com segurança, minimizando os riscos e maximizando a segurança do código e das aplicações.

Praticas para processo de desenvolvimento seguro

- A pratica seria baseada no projeto OWASP para o processo de desenvolvimento seguro. Devido ao êxito em projetos onde o OWASP foi implantado, ao grande uso no mercado e se tratar de uma comunidade gratuita e aberta que conta com uma gama gigante de especialistas de segurança WEB, os níveis de conhecimento, ferramentas, processos e testes é altíssimo e torna a implantação menos burocrática e difícil.

Danos e mitigação do Zé Connect

- Vejo 2 danos sendo só principais para esse produto, sendo eles reputação da empresa e aplicação de multa devido a incidentes de vazamento de informação previstos da LGPD.
    - Reputação: casos de ataques hackers ou vazamento de informações, tem causado aos usuários dos serviços, bem como parceiros, grande desconfiança e falta de credibilidade

ao usar serviços ou comprar produtos de uma empresa, ocasionando debandada de possíveis parceiros de negócios e clientes. Dano incalculável;
    - LGPD: sabemos hoje que a lei multa as empresas que tenham incidentes de vazamento de informação, em 2% do faturamento da empresa limitando ao valor de R$ 50 milhões por incidente. Mesmo conseguindo comprovar que todos os controles possíveis ao negócio foram implantados, tais como ferramentas, processos e pessoas, a multa ainda pode acontecer e o fato de ter que notificar a ANPD (Autoridade Nacional de Proteção de Dados) ocasiona não só o prejuízo da multa, também o prejuízo de reputação.
- Para evitar que esses danos ocorram, vamos investir em ferramentas e processos de gerenciamento, exemplificando o uso do DLP para evitar vazamento de informações vindo do público interno da empresa e as ferramentas de proteção da estrutura da aplicação, com o uso do WAF, DBF, EDR e SIEM e contar com a equipe de SOC fazendo o gerenciamento dos incidentes e contando com a equipe de resposta a incidentes para mitiga-los.

Caso infeliz...

- Formas de investigar o dado vazado:
    - Através do gerenciamento do DLP, analisaria os incidentes de vazamento de informação que foram gerados, tentando validar qual usuário tratou determinado dado sensível e para onde esse dado foi enviado;
    - Também através dos log's do banco de dados, analisando quais tipos de transações foram realizadas e por qual usuário foi feito, visando encontrar o dado sensível vazado através de alguma transação;
    - E investigar na solução de PAM as sessões feitas ao sistema e banco de dados, buscando por comandos que deem indícios que possam identificar o autor do vazamento da informação e qual a informação vazada;
    - Analise localmente no SYSLOG (servidor de log's centralizado) buscando informações que sejam sensíveis armazenadas no servidor ou em algum log armazenado nele.
- Após identificação do dado sensível vazado, providenciaria de imediato a inclusão desses dados em uma política do DLP, evitando que os endpoints corporativos façam uso daquele dado fora da corporação;
- Providenciaria a exclusão do dado sensível do SYSLOG e a remoção do backup da data a qual a informação foi salva no SYSLOG, evitando que um restore de backup gere um novo incidente de vazamento de informações;
- Após identificação do autor do vazamento da informação, validaria com time de compliance e jurídico, as sanções previstas para o usuário autor do incidente. Em casos de se tratar com educação corporativa, pois pode ter sido um engano, falta de maturidade ou conhecimento técnico que veio a ocasionar tal incidente, verificaria junto ao time de RH sobre um possível treinamento ou processo de educação do usuário para evitar casos futuros e, caso aconteça novamente, tomar as medidas cabíveis.