Modelagem de ameaças

**Nome da aplicação: RH**

**Módulos:** Organograma, Gestão de desempenho (W3), Beneflex, Composição de efetivos, aniverserintes

**Recursos valiosos**

Quais são os recursos valiosos da aplicação? (Isso pode variar desde dados confidenciais, tais como bancos de dados de pedidos dos clientes, até suas páginas da Web ou disponibilidade do site)

Dados de todos colaboradores, benefícios, informações financeiras dos colaboradores

**Resumo de arquitetura**

O que faz a aplicação?

Sistema de gerenciamento de recursos humanos.

Aplicação envia dados para sistemas externos? Não E interno? Sim. Para o APDATA

Aplicação recebe dados para sistemas externos? Não E interno? Sim, recebe do APDATA

Aplicação é pública ou interna? Aplicação interna.

Descrição do APDATA: Aplicação de terceiro, não desenvolvida pelo cliente.

Resumo de arquitetura (Desenhar se necessário):

Sem criptografia

APDATA

RH  
(Módulos)

Acesso   
Navegador

SQL  
Server

Autenticação  
LDAP/AD

Sem criptografia

Quais são as tecnologias? (Ex.: Banco de dados, tráfego de rede, aplicações dependentes)

|  |  |
| --- | --- |
| **Tecnologia / Plataforma** | **Detalhes da implementação** |
| Banco de dados | SQL server |
| Tráfego de rede | Não há criptografia para comunicação com APDATA |
| FrontEnd | ASP Clássico + VB6 + .dot 2.3 + aspnet + c# |
| Backend | Não se aplica |
| Autenticação | LDAP/AD |
|  |  |

**Validação de entrada**

Todos os dados de entrada estão validados? É utilizado um escape de dados padrão da linguagem. Não há validadores customizados

Um invasor poderia injetar comandos ou dados maliciosos na aplicação? Sim. Ameaça interna.

Os dados são validados enquanto passam entre limites de confiança separados (pelo ponto de entrada recebedor)? N/A

Os dados do banco de dados podem ser confiáveis? Não. Dados com má formação podem ser imputados.

**Autenticação** (É gerenciado pelo LDAP/AD)

As credenciais estão seguras se passarem pela rede?

As diretivas fortes de segurança são utilizadas?

As senhas fortes são reforçadas?

Você está usando certificados?

Os verificadores de senha (que usam hash de mão única) são usados para as senhas dos usuários?

**Autorização** (É gerenciado pelo LDAP/AD)

Quais guardiões estão sendo usados nos pontos de entrada da aplicação?

Como a autorização é reforçada no banco de dados?

A estratégia de defesa profunda está sendo usada?

Você obtém falhas seguras e somente permite acesso sob confirmação bem-sucedida de credenciais?

**Gerenciamento da configuração** (Não se aplica para essa aplicação)

Que interfaces de administração a aplicação suporta?

Como elas são protegidas?

Como a administração remota é protegida?

Quais armazenamentos de configuração são usados e como eles são protegidos?

**Dados sensitivos**

Que dados sensitivos são controlados pela aplicação? Dados pessoais

Como eles são protegidos pela rede e armazenamentos persistentes? Não há proteção

Que tipo de encriptação é usado e como suas chaves são utilizadas? Não é realizada a criptografia em frontend, essa função é encarregada do módulo intermediário.

**Gerenciamento da sessão**

Como as cookies de sessão são geradas? Beneflex – Composição de efetivos – Pelo próprio .net.

Como elas são protegidas para prevenir roubos? N/Q

Como o estado persistente de sessão é protegido? N/Q

Como o estado de sessão é protegido quando ele cruza a rede? N/Q

De que forma a aplicação autentica com o armazenamento de sessão? N/Q

As credenciais passam pela rede e são mantidas pela aplicação? Em caso afirmativo, de que forma elas são protegidas? N/Q

**Criptografia** (Não se aplica para essa aplicação)

Quais algoritmos e técnicas criptográficas são usados?

De quanto tempo são as chaves de encriptação e como elas são protegidas?

A aplicação coloca em ação a sua própria encriptação?

Com que freqüência as chaves são recicladas?

**Manipulação do Parâmetro**

A aplicação detecta parâmetros falsificados? Não

Ela valida todos os parâmetros em campos de formulários, estado de áreas de visão, dados de cookie e cabeçalhos http? Não

**Gerenciamento de Exceção**

Como a aplicação controla condições de erros? Emite mensagem de falha de genérica

As exceções têm sempre permissão para voltar ao cliente? N/Q

As mensagens genéricas de erros que não contêm informações exploradas são usadas? N/Q

**Auditoria e logging**

A sua aplicação auditora atividades através de todas as camadas em todos os servidores?

Os logs são internos do “Job”. Não tem probabilidade de dados sensíveis serem gravados em arquivo de log.

Como são protegidos os arquivos de log? N/a

**Outros:**

Privilégios: Sistema Beneflex possui dois perfis (Colaborador e RH)

Números randômicos: Não

Manipulação de arquivos: Beneflex exporta relatórios em PDF e Excel. Não há importação de arquivos para o sistema.

**Possíveis ameaças da aplicação**

* Usar validação pobre de entrada que leva ao cross-site scripting (XSS), injeção de SQL e ataques de estouro de buffer.
* Passar credenciais de autenticação ou cookies pelos links não criptografados da rede, o que pode levar ao roubo ou captura de credenciais.
* Armazenar segredos de configuração, tais como strings de conexão e credenciais de conta de serviço, em texto puro.
* Usar processo sobre privilegiado e contas de serviço.
* Usar técnicas inseguras de códigos de acesso aos dados, o que pode aumentar as ameaças à injeção SQL.
* Contar com a integridade de parâmetros passados do navegador, por exemplo, de campos de formulários, strings de consultas, dados de cookie e cabeçalhos HTTP.
* Usar tratamento inseguro de exceções, que podem levar a ataques de negação de serviço e divulgação de detalhes em nível de sistema, úteis para o invasor.