NORMA DE GESTÃO DE VULNERABILIDADE

1. INTRODUÇÃO

Essa norma de segurança da informação, vem para complementar a Política de Segurança da Informação, definindo as diretrizes para a proteção dos ativos e serviços de informação da Elubel.

2. OBJETIVO

Esta norma tem como objetivo orientar e dar as diretrizes do que analisar para adquirir um antivirus e o como proceder em relação a realização do scan de vulnerabilidade e teste de invasão. Tendo como objetivo prevenir a exploração de vulnerabilidades no ambiente corporativo.

3. ABRANGÊNCIA

Todos os colaboradores que atuarem no suporte, infraestrutura ou segurança da informação na Elubel deve seguir esta norma.

4. ANTIVÍRUS

4.1. Tipo de antivírus

O antivírus deve ter como característica:
Segurança Web, bloqueio de downloads e códigos maliciosos, controle de uso de mídias externas (USB, CD, Drive Externo, Bluetooth), ser capaz de detectar e erradicar todas os tipos de infecção conhecidos, proteção em tempo real, ter controle centralizado, FIM, DLP, HIPS, agendamento de scan e logs de auditoria.

4.2. Privilégios de usuários

4.2.1. A console do antivírus deve fornecer a opção de criar vários níveis de acesso ao gerenciamento da aplicação.
4.2.2. A conexão no console deve expirar diante da inatividade do operador.
4.2.3. O agente do antivírus instalado nos hosts deve ter bloqueio de alteração e desinstalação por pessoas não autorizadas.
4.2.4. Somente pessoas autorizadas deve gerenciar o antivírus, seja ele na console de gerenciamento ou no host.
4.2.5. A senha de acesso a console ou de desativação do agente do antivírus, não deve ser fornecido a ninguém que não seja da equipe de segurança e/ou suporte.
4.2.6. Caso seja necessário desativar o antivírus ele deve ter capacidade de se auto iniciar após um curto período.
4.2.7. O usuário é proibido de transferir dados de cartão para dispositivos removíveis.

4.3. Periodicidade de atualização

4.3.1. A console do antivírus deve estar apta a receber sempre todas as atualizações da fornecedora (Aplicação, banco de assinaturas e vacinas) automaticamente.

4.3.2. O agente do antivírus nos hosts deve estar apto a receber automaticamente todas as atualizações fornecidas pela console, exceto atualização do agente que deve ser aplicada de forma manual seguindo os parâmetros descrito no documento Baseline do Antivírus.

4.3.3. A atualização de vacina nos agentes não pode ser superior a 10 minutos.

4.3.4. A atualização de software do agente deve ser feita frequentemente seguindo **Baseline do Antivírus**

4.4. Periodicidade das varreduras automáticas

O antivírus deve trabalhar fazendo scan em tempo real, além de fazer uma verificação completa pelo menos três vezes na semana.

4.4.1. As funções de proteção em tempo real e detecção com base no comportamento devem estar habilitadas para todas as estações de usuários e dispositivos móveis.

4.4.2. Sites, serviços e arquivos baixados da internet detectados como possíveis ameaças serão automaticamente bloqueados em estações de usuários dispositivos móveis e servidores corporativos.

4.4.3. As verificações completas em servidores deveram ser feitas em horário de baixa demanda.

4.4.4. Caso um servidor corporativo esteja infectado ou com suspeita de infecção de código malicioso, deverá ser adotadas medidas para garantir o isolamento dele da rede corporativa e da internet, levando em consideração o impacto dessa ação e efetuar as devidas mitigações.

4.4.5. Caso uma estação de trabalho ou dispositivo móvel esteja infectado ou com suspeita de infecção de código malicioso, o mesmo deverá ser isolado da rede e trabalhar nas devidas mitigações.

4.5. Gestão do antivírus

Diariamente é necessário revisar a console do antivírus para verificar se não existe nenhum alerta para ser corrigido, caso possua alguma notificação tem que fazer o tratamento imediato do incidente.

5. SCAN DE VULNERABILIDADE

5.1. Buscando sempre aperfeiçoar a segurança e mitigar os ricos a equipe de segurança deve utilizar uma ferramenta de scan de vulnerabilidade devidamente atualizada.

5.2. A varredura de vulnerabilidade interna deve ocorrer pelo menos mensalmente, por um profissional qualificado ou entidade especializada em varredura de vulnerabilidade.

5.3. A varredura de vulnerabilidade interna deve ser feita de forma autenticada, a modo de obter um relatório mais aprofundado e detalhado de possíveis vulnerabilidades.
5.4. A varredura de vulnerabilidade externa deve ocorrer pelo menos semestralmente.
5.5. Executar varredura interna e/ou externa sempre que necessário ou após qualquer mudança no ambiente.
5.6. Toda Vulnerabilidade encontrada deverá ser tratada, evitando assim que ela se torne uma vulnerabilidade maior no futuro. Todo tratamento de ameaça deve obedecer a ordem do mais grave, para o menos grave.
5.7. Toda vulnerabilidade deverá ser gerado um documento de resposta a incidente e registrar um chamado se assim disponível. No qual se deve descrever a solução e status da vulnerabilidade.
5.8. Após promovidas as correções, deve-se realizar novos testes com a finalidade de comprovar a efetividade das correções.
5.9. A prioridade da tratativa das vulnerabilidades deve ser sempre do mais crítico, para o menos crítico.
5.10. As evidências das varreduras de vulnerabilidades e correções devem ser documentadas e guardadas**.**

6. PENTESTS

6.1. A execução de Testes de Penetração deve ser realizada no mínimo duas vezes ao ano ou quando houver uma mudança significativa do ambiente. O processo deve ser realizado por uma empresa terceira de comprovada idoneidade, que tenham profissionais comprovadamente capacitados.
6.2. Os testes de penetração devem comprovar a eficácia dos controles de segmentação.
6.3. Ao fim do Teste de Penetração deve ser gerado um relatório identificando o que foi feito, como foi feito, quando foi feito, vulnerabilidades, evidencias e sugestões de remediação.
6.4. O escopo do Teste de Penetração deve ser todos os ativos (servidores, sites etc.).
6.5. O Teste de Penetração deve seguir metodologias reconhecidas internacionalmente pela área de segurança da informação.
6.6. O Teste de Penetração feito pela própria equipe poderá ser realizado periodicamente desde que se tenha alguém capacitado para fazer e com a devida aprovação da empresa.
6.7. O Teste de Penetração feito pela própria empresa não substitui a contratação de um terceiro para realizar o procedimento ao menos 2 vezes ao ano.
6.8. Todas as vulnerabilidades encontradas no Teste de Penetração que forem exploráveis devem ser analisadas e corrigidas imediatamente. Após promovidas as correções, deve-se realizar novos testes com a finalidade de comprovar a efetividade das correções.
6.9. As correções efetuadas baseadas no relatório de Teste de Penetração devem ser documentadas e guardada.

7. OBSERVAÇÃO DE EVOLUÇÃO DOS MALWARES

Deve-se analisar sempre os logs de auditoria referente aos malwares, e outras ameaças, para entender onde estão as principais vulnerabilidades do ambiente e poder atuar de maneira preditiva e preventiva, para diminuir as ocorrências visando evitar as atuações corretivas.

8. OBTENÇÃO DE INFORMAÇÃOS DE FONTES CONFIÁVEIS

A equipe de segurança e infraestrutura deve sempre buscar informações referentes a segurança da informação, vulnerabilidades, atualizações, ameaças, mitigações e outros. Essas informações devem vir de fontes confiáveis, como algum fornecedor atual de segurança, Sistema Operacional e empresas especializadas.

9. DETECÇÃO DE MUDANÇA

Arquivos críticos devem ser constantemente monitorados por ferramentas de detecção de mudança, para analisar em tempo real se houve alteração, acréscimo e/ou exclusão de algum arquivo.

Arquivos críticos só poderão ser modificados com autorização, caso contrário a ferramenta de monitoramento de integridade do arquivo deve alertar os administradores do sistema do ocorrido.

Ao ser notificado por uma alteração não autorizada a equipe de suporte, infraestrutura e/ou segurança devem agir imediatamente para analisar o caso e fazer as devidas tratativas.

10. SENHA CRIPTOGRAFICA

A senha da criptografia de dados pessoais como cartão de crédito, deve ser alterada periodicamente no intervalo de até doze meses, ou quando um funcionário com poder da senha for desligado.

11. SANÇÕES E PUNIÇÕES

O descumprimento dessa norma pode acarretar sanções e punições aos envolvidos.

12. REVISÕES

Esta norma deverá ser revisada anualmente ou extraordinariamente, a qualquer momento se for necessário.