Giovanni de Aguirre Tamanini

ContaTudo Ltda.
Análise de maturidade e proposta de melhorias quanto à segurança da informação

Florianópolis

17 de outubro de 2022

Giovanni de Aguirre Tamanini

ContaTudo Ltda.
Análise de maturidade e proposta de melhorias quanto à segurança da informação

Trabalho apresentado à disciplina Fundamentos de Segurança da Informação do Senai/SC.
Professor: Edinaldo Moraes

Senai / SC

Graduação em Análise e Desenvolvimento de Sistemas

Florianópolis

17 de outubro de 2022

Sumário

1 Problemática e escopo do relatório

Para a análise de maturidade e desenvolvimento de melhorias quanto à segurança da informação da empresa analisada, faz-se necessário inicialmente a ordenação das informações mais importantes, incluindo toda a problemática conhecida, como se segue:

- Empresa: ContaTudo Ltda.
- Atuação: prestação de serviços de contabilidade.
- Informações/dados dos clientes:
    1. Nome completo.
    2. Dados bancários corporativos ou de pessoas físicas.
    3. Pagamento de notas fiscais de serviços de segurança patrimonial.
    4. Contratos.
    5. Outros.
- Problemática: empresa familiar que lida com informações importantes e confidenciais dos clientes e nunca se preocupou com segurança física, segurança da informação ou privacidade de dados. Pontualmente, podem vir a ser considerados problemas:
    1. Sobrinho do dono da empresa faz esporadicamente o papel de funcionário de TI.
    2. PC na recepção até então pouco utilizado é responsável pela segurança da rede local.
    3. Firewall baseado em Linux é utilizado neste PC.
    4. É utilizado um antivírus gratuito e cheio de propagandas de terceiros nesta máquina "responsável"pela segurança.
    5. Arquivos em papel em pastas são armazenados nas gavetas de duas pessoas.
    6. Uma das pessoas responsáveis pelos arquivos físicos é estagiária de contabilidade, mas o curso de graduação dela é em outra área do conhecimento que tem pouco ou nada a haver com contabilidade.

Como escopo do relatório desenvolvido a seguir tem-se:

- Identificar as principais vulnerabilidades quanto à segurança da informação na empresa;

- Propor melhorias ou novas abordagens (possíveis de serem implementadas observando o custo-benefício) para os itens identificados conforme a norma ISO27001 e a Lei Geral de Proteção de Dados.

2 Análise das vulnerabilidades e sugestões de melhorias

2.1 Quanto à segurança em recursos humanos

Analisando a atual condição da empresa e de seus funcionários, percebeu-se que as medidas que deveriam ser tomadas antes de um funcionário efetivar-se no cargo (conforme a ISO/IEC 27001, anexo A.7), não foram levadas em conta. Um dos responsáveis pela segurança de TI é sobrinho do dono da empresa, e realiza algumas atividades esporadicamente, não é contratado da empresa. O mesmo foi responsável pela implementação do único sistema de segurança da empresa, um Linux *firewall* em um computador que já possui algumas questões que devem ser corrigidas. Outra funcionária (estagiária), responsável por arquivos físicos e outras questões da área de contabilidade, está fazendo graduação em outra área do conhecimento, não sendo a área de ciências contábeis ou correlatas.

Quanto a prestação de serviço do sobrinho, é necessário que estas decisões técnicas de rede e segurança sejam determinadas por um profissional da área de TI. Ou seja, todas as vezes que a empresa necessitar, contratar uma consultoria especializada para tal. Não é necessária a contratação permanente de um profissional da área, a não ser que seja inevitável por falta de mínima mão de obra com a devida qualificação. A seguir no tópico *Quanto à segurança nas operações e comunicações*, serão elencadas as vulnerabilidades técnicas já existentes e melhorias para os problemas específicos.

Para a estagiária, é necessário analisar se a mesma está desempenhando bem sua função, ou seja, se mesmo em área de formação completamente diferente, a mesma consegue desempenhar bem suas atividades. A empresa pode a partir de agora treinar a funcionária para exercer bem sua função, adotando sugestões que serão dadas na seção *Quanto à segurança física*. Finalizando o período de estágio e sendo avaliado o desempenho, se preciso, contratar alguém da área e começar a adotar as sugestões desde o início.

Por fim, principalmente, adotar segundo a norma ISO/IEC 27001, um Sistema de Gestão de Segurança da Informação, e escolher um responsável (de preferência o dono ou pessoa de confiança da empresa que estabelecerá uma PSI) que possa gradativamente se especializar nestas questões e adequar/atualizar a empresa quanto aos requisitos do SGSI, que são:

1. Contexto da organização
2. Liderança (PSI - política de segurança da informação)
3. Planejamento

4. Apoio
5. Operação
6. Avaliação do desempenho
7. Melhoria

2.2 Quanto à segurança física

De acordo com a norma ISO/IEC 27001 (anexo A.11), a segurança física e do ambiente também deve ser repensada para a empresa. A mesma não possui nenhum sistema de controle de entrada física e nenhum controle para a segurança do perímetro físico da instalação. Sugere-se a instalação de câmeras de segurança CCTV na entrada e área de atendimento ao cliente, assim como em áreas onde existam arquivos físicos que contenham informações confidenciais da empresa e dos clientes. Um *kit* de alarme também deve ser instalado para proteger o acesso à empresa em horário não comercial.

Como comentado na seção *Quanto à segurança em recursos humanos*, os arquivos físicos são guardados em gavetas de funcionários. Sugere-se que estes arquivos sejam guardados à chave em local específico para tal, para que se tenha controle do acesso a essas informações de forma organizada e segura.

O computador responsável pelo *firewall* da rede local da empresa não deveria estar na recepção. Aconselha-se um espaço mais reservado onde um dos funcionários (com conhecimento em TI e redes mais avançado) possa ser responsável pela administração da rede. Se for necessário e possível, sugere-se fazer uma reestruturação da rede local com o uso de um *firewall* do tipo Fortigate da Fortinet (hierarquia –> *firewall* » roteador » *switches* » etc), pois são 12 funcionários, portanto pelo menos 12 computadores mais celulares vulneráveis.

2.3 Quanto à segurança nas operações e comunicações

Segundo a norma ISO/IEC 27001 (anexos A.12 e A.13), a proteção contra *malware*, e uma solução para a empresa ter cópias de segurança de suas informações é muito importante. Recomenda-se o uso de um antivírus como o Endpoint Security Cloud Plus da Kapersky que oferece prevenção de *ransomware* e muitas outras funcionalidades. Além disso recomenda-se o uso de um servidor com o Windows Server 2022 instalado, como *backup*.

Referências

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION / INTERNATIONAL ELECTROTECHNICAL COMMISSION. *ISO/IEC 27001*: Sistema de gestão da segurança da informação. Brasil, 2013. 30 p. Citado 2 vezes nas páginas 5 e 6.