1- Introdução

A segurança de informação atualmente é a parte vital de qualquer empresa, proteger seus recursos tecnológicos significa defender o físico e financeiro, assim como sua reputação no mercado e os funcionários. A definição de normas e políticas de segurança da informação deve ser a primeira ação que toda a organização deveria executar para se proteger de riscos de segurança (PELTIER, 2012). Com isso, podemos então, observar dentro de toda corporação que lida com dados, domínios de segurança de informação, sendo estes por sua parte subdivisões da área, separados em categorias.

A empresa Votorantim, organização de diversos segmentos, incluindo a siderurgia, por exemplo, utiliza dos domínios apontados no parágrafo acima. Conta com uma área direcionada à informação, tratando dados de produção, gestão de negócios e pessoas. Esses dados de produção são retirados de *softwares* ERPs e enviados a um banco de dados, que se juntam com os dados de gestão e da área de pessoas, que por sua vez são inseridos no sistema através de plataformas que são direcionados aos gestores e ao time de recursos humanos, que realiza o controle financeiro empresarial, contratações e desligamentos de dentro da corporação.

As empresas contam com rede de computadores que engloba cada setor, que possuem diferenças entre eles, como por exemplo: os gestores da produção não possuem visão do que o recurso humano está administrando, porém todos os setores conversam entre sim, como a gestão possui visão de como procede a produção, mas cabe aos gerentes de produção coordenar como os operadores vão atuar em seus postos de trabalho.

A seguir será detalhado como são os domínios de segurança da informação da organização Votorantim, separadamente por categoria:

2- Domínios

2.1 Domínio do Usuário

Tratando-se do elo mais fraco da corrente de segurança da informação, a organização planejou formas de impedir que usuários sem credenciais acessem os dados. Para acessar as instalações da empresa é necessário possuir crachás de identificação que conta com nome, foto e função do funcionário, o crachá também é identificado através de uma tarja magnética e deve ser utilizado também por quem visita a empresa. Neste caso, as informações da pessoa ficam contidas na tarja magnética e o indivíduo não pode andar livremente pelas instalações, apenas acompanhando um funcionário.

Não sendo apenas dessa maneira, prestadores de serviços, não contam com acesso a rede, para possuir acesso a computadores e utilizá-los, devem ser funcionários registrados, contar com autorização do administrador da rede, possuir login e senha. Ainda assim, existem níveis hierárquicos, que bloqueiam, por exemplo: operadores de terem acesso a dados que convém apenas a gestores. E restringe setores a receberem informações de outras áreas da empresa.

2.2 Domínio dos Dispositivos

Uma forma encontrada de prevenir ameaças externas é o bloqueio a páginas de caráter duvidoso, que podem possuir *malware* prontos para realizar ataques a computadores. O monitoramento da rede é constante, supervisores mantém sistemas de vigilância para cada terminal com acesso à internet. Os *downloads* são restritos apenas aos e-mails da aplicação cadastrada e permitida no sistema.

Também para restringir o acesso a rede interna, apenas terminais registrados podem se conectar para que não haja a tentativa de acesso através de equipamentos inseguros, terminais operacionais que comandam equipamentos e máquinas não estão ligados a rede global de computadores (*internet)*.

2.3 Domínio da Rede Lan

Para manter a segurança os *datacenters* não são locais, são localizados em grandes hospedagens externas, pois, assim ocorre uma economia financeira por parte da segurança dos dados. Porém, a porta da rede não costuma ser verificada, não restringindo o acesso de códigos maliciosos à rede, comprometendo a segurança. Testes de penetração não são realizados com a devida periodicidade, restando a dúvida se a rede é ou não inviolável.

No que diz respeito a rede *Lan,* muitas camadas de segurança são quebradas, o que compromete as seguidas. A criptografia não é utilizada para a transferência de todos dados, apenas caso sejam enviados por e-mails.

Mesmo com todas as falhas já citadas, é difícil o acesso a rede interna, programas e aplicativos não podem ser instalados nas máquinas das empresas e o sistema operacional está sempre atualizado e corrigido para falhas de segurança.

2.4 Domínio de Nuvem Privada (*WAN*)

Já no caso da nuvem privada, as instalações contam com roteadores configurados para a melhor segurança, sem senhas padrões e apenas de conhecimento dos administradores da rede. Além de contar com atualizações frequentes que corrigem falhas, os testes não são conduzidos com a periodicidade que deveria, então é desconhecido o nível de proteção dos equipamentos.

Mesmo os usuários remotos que possuem *notebooks* ou *smartphones,* não possuem permissões para baixarem arquivos utilizando a rede interna. Contudo, é possível acessar qualquer site usando dispositivos móveis, porém, compromete parte da segurança já que uma camada que permite esse acesso dos usuários a sites duvidosos está sendo quebrada.

2.5 Domínio de Nuvem Pública

Quando uma empresa que não se enquadra no setor de tecnologia, as políticas de segurança da informação não são atualizadas a alguns anos, proporcionando a quebra de camadas de segurança. Os cursos e os ensinos na área de segurança não são passados aos funcionários, tornando o elo fraco ainda mais fraco, ocorrendo brechas por causa da engenharia social, que atua diretamente com os funcionários em questão.

Apesar disso, as senhas possuem limites de tempo para serem utilizadas, que em determinados períodos expiram e devem ser trocadas obrigatoriamente, não podendo repeti-las, não usar dados pessoais dos usuários e possuindo um limite mínimo de 8 caracteres. Torna-se complexo e quase inviável a quebra por força bruta das senhas. Autenticação de múltiplos fatores não são obrigatórias, algo que deveria ser um comprometimento da empresa para com seus funcionários, porém fica a critério do usuário da conta utilizar ou não a dupla autenticação.

2.6 Domínio de Instalações Físicas

Para o acesso às instalações prediais é necessário o uso de credenciais, já explicadas acima, que dificultam seus acessos. Além disso, *datacenters* e servidores não se localizam na matriz da empresa, e sim em grandes *hosts* distribuídos. Assim, podendo economizar uma quantia monetária em instalações físicas, dessa maneira, permitindo o acesso quase que ininterrupto aos dados.

Mesmo assim, dentro da empresa encontram-se geradores de energia com prevenção de possíveis quedas energéticas, sistemas de CCTV (do inglês: *closed-circuit television*, que significa **circuito fechado de televisão**) para observações das instalações, para prevenção de roubos de *hardware*, os terminais operacionais ficam instalados em caixa com cadeado e as chaves de acesso são encontradas apenas com administradores da rede.

2.7 Domínio de Aplicação

Como o acesso aos servidores já se torna restrito por não ser um *datacenter* local, previne as falhas de seguranças nos sistemas operacionais ligados à *internet*. *Patchs* de correção e atualizações são executados com periodicidade, automaticamente nas máquinas, assim, mantendo afastado problemas com obsolescência do *software*.

Os dados mais sigilosos, não ficam salvos nas máquinas locais, para que, em caso de perdas, não haja grandes danos. Além disso, os *backups* são ligados diretamente ao servidor de arquivos. Os equipamentos novos compram com protocolos de seguranças que permitem ou restringem se a máquina é segura para o uso.

Conclusão

Em suma, é visto que dentro das instalações existem padrões que são seguidos para a restrição de seus acessos, não permitindo no seu interior de dados, que pessoas mal intencionadas possam ter acesso. Conclui-se que: dados sigilosos das empresas em questão, estão de certa forma seguros, pois, a responsabilidade de armazenar, proteger, manter o acesso constante e sua redundância é de um terceiro.

Mesmo que ocorram falhas dentre as camadas de segurança, elas irão existir até que ocorra um investimento nesse âmbito, mostrando para os funcionários os modelos de segurança que devem ser seguidos, diante das novas tendências em relação aos dados da corporação, que prevê possíveis perdas e não recuperação.