SEGURANÇA CIBERNÉTICA EM ORGANIZAÇÕES DISTRIBUÍDAS: ESTUDO DE CASO DA SOLUÇÃO IMPLEMENTADA EM UMA INSTITUIÇÃO PÚBLICA

GONÇALVES, E. L. O.; AMARAL[1], J. B. T.; BRUSAMOLIN, V.; ZAMPIERI, J. A.

RESUMO

RESUMO - Este artigo investiga como procedimentos, hardware e software podem ser integrados, a fim de oferecer segurança contra invasões e ataques hackers, ou seja, defesa cibernética, em sistemas de comunicação de dados em organizações distribuídas. Um estudo de caso foi realizado em uma organização pública composta por vinte e duas filiais interligadas, que teve a necessidade de projetar e implantar uma solução de segurança. Como resultado, obteve-se uma solução arquitetônica satisfatória e uma série de procedimentos que podem ser adaptados a outras organizações que desejam implantar práticas de segurança da informação.

Palavras-chave: Segurança da Informação. Controle de Acesso. Defesa Cibernética.

Cyber security in distributed organizations: a case study of the solution implemented in a public institution

ABSTRACT

ABSTRACT - This article investigates how hardware and software can be integrated in order to provide security against intrusions and attack, i.e. cyber defense, in data communications systems in distributed organizations. A case study was carried out upon a public organization which is composed by twenty-two interconnected branches that had the need for designing and deploying a security solution. As a result, a satisfactory architectural solution and a series of procedures that can be adapted to other organizations wishing to deploy information security practices were obtained.

Key words: Information Security. Cyber Defense. Access Control.

1 INTRODUÇÃO

A evolução dos dispositivos de telecomunicações e de informática proporcionou uma facilidade de comunicação interpessoal sem precedentes. A distância já não constitui um obstáculo ao usuário, pois lhe é indiferente se a comunicação eletrônica ocorre com uma pessoa nas proximidades ou no outro lado do planeta. A tecnologia aparenta igualar as distâncias mediante o veloz transporte de grandes volumes de informação na forma de dados, voz, imagem e vídeo.

As organizações passaram a aproveitar tais tecnologias como mecanismo de comunicação,

[1] C-eletrônico: joao.tsuruda@gmail.com.

reduzindo custos e aumentando a quantidade e velocidade das mensagens. A interligação das diferentes instalações de uma grande organização, ou da organização com seus clientes e fornecedores, geralmente só é economicamente viável com o uso da rede mundial de computadores, a Internet, um vasto espaço digital em que milhões de entidades trocam informações.

O uso da infraestrutura compartilhada da Internet, entretanto, possibilita que vulnerabilidades tecnológicas sejam exploradas por estelionatários, fraudadores, hackers e criminosos em geral, lesionando tanto as finanças quanto a imagem de organizações. Nesse contexto, a comunicação segura é essencial, pois além da necessidade de preservar seus dados e segredos comerciais, dispositivos legais as obrigam a proteger informações de seus funcionários, parceiros e clientes.

Como combinar equipamentos, políticas e técnicas de segurança de forma adequada para proteger a rede de comunicações de dados de uma organização, com diversas instalações interconectadas pela Internet? O presente artigo compartilha uma sequência de passos e a solução arquitetural adotada em uma instituição que possui 22 (vinte e duas) instalações interligadas por rede de dados, que tem apresentado resultados satisfatórios. Entende-se que as técnicas podem ser adaptadas para outras organizações que desejem adotar práticas de proteção informacional.

2 METODOLOGIA

Foi realizado o estudo de caso em uma organização que possui filiais interligadas, em que foi implantada uma solução de segurança da informação para bloquear os crescentes ataques aos seus sistemas de comunicações de dados. Os técnicos responsáveis pela concepção da solução foram entrevistados. A partir das entrevistas, elaborou-se uma descrição das atividades executadas, enfatizando os aspectos arquiteturais.

O embasamento teórico apresenta o resultado de uma pesquisa documental sobre os conceitos básicos utilizados pelos profissionais no desenvolvimento dos trabalhos.

3 EMBASAMENTO TEÓRICO

Aparatos tecnológicos empregados na TI e relacionados à Segurança da Informação

A implementação de práticas de segurança da informação é realizada por meio da correta instalação e configuração de equipamentos que suportam os requisitos, por intermédio de uma série de comportamentos e protocolos. A seguir, uma lista de equipamentos, protocolos e conceitos que, utilizados nas redes de computadores, materializam os comportamentos, modos de operação, agregados lógicos e administrativos necessários a uma instalação segura:

- **IPS - Intrusion Prevention System:** sistema de detecção que identifica tentativas de invasão na rede e encerra a conexão suspeita. Geralmente utiliza um banco de dados com assinaturas de ataques já conhecidos.
- **IDS - Intrusion Detection System:** sistema de detecção que busca identificar anomalias na rede causadas por invasores. Gera alertas após a rede já haver sido invadida.
- **Firewall:** "dispositivo de segurança, que visa realizar a filtragem daquilo que é ou não permitido ser acessado em uma rede, seja o acesso proveniente da rede interna ou da rede externa". Nesse equipamento, o bloqueio é realizado por endereços ou portas específicas, por tipo de pacotes ou por tipo de protocolo. Para que seja eficaz, todo o tráfego originado ou destinado à rede protegida deve ser obrigado a atravessá-lo.
- **Segmentação de redes:** considerando um grupo de máquinas arbitrariamente grande, na casa das centenas ou milhares, interligados na mesma rede lógica. A quantidade de colisões de pacotes e de broadcast resultante poderá causar lentidão ou mesmo impossibilitar a operação da rede. Outra desvantagem resultante é a facilidade de comunicação direta entre as máquinas, criando um ambiente perfeito para a disseminação de vírus, worms e outros malwares. Ao segmentar os

computadores em grupos lógicos pela configuração de rede, diminuem-se as colisões e obrigam-se os pacotes a atravessar um roteador para alcançar outro grupo. É proporcionada por meio de roteadores que podem conter ACL[2]s determinando o tipo de tráfego aceitável de um grupo para outro.

- **Proxy HTTP:** servidor que recebe as requisições destinadas à Internet e, após submeter a análise de suas ACL, encaminha o pedido ao website externo. A resposta normalmente ficará em cache, de forma que as consultas subsequentes ao mesmo destino serão imediatamente atendidas, sem necessidade de nova consulta ao website. Esse mecanismo proporciona grande velocidade de acesso ao usuário final e economia de recursos no link de acesso.
- **UPS (Uninterruptable Power Supply):** fonte de energia ininterrupta; no Brasil é popularmente chamada de "nobreak".
- **Servidor de Máquinas Virtuais (hospedeiro):** sistema operacional ou módulo que propicia melhor utilização da capacidade do hardware existente, no qual um único servidor físico pode hospedar diversas máquinas virtualizadas, inclusive com sistema operacionais diferentes. A utilização de máquinas virtuais apresenta diversas vantagens na operação:
  - É possível criar "clones" de máquinas virtuais com um simples comando. Esse clone pode ser utilizado para homologar uma correção e/ou atualização antes de aplicá-la no sistema em produção, sem causar paradas desnecessárias, ou mesmo para gerar o *backup* de um sistema inteiro em poucos segundos.
  - Possibilita a migração das máquinas virtuais de um hardware a outro, mesmo sem a interrupção dos serviços, permitindo fazer a manutenção no hardware de servidores sem interromper a produção.
  - Todos os servidores são instalados em um único tipo de hardware, padronizado pela máquina virtual.
  - O aproveitamento do *hardware* existente, a economia de espaço físico em *racks* e ar condicionado propiciam significativa redução de custos de operação.
  - É possível executar vários sistemas operacionais no mesmo equipamento simultaneamente.
  - As ferramentas de gerenciamento permitem redução de tempos de parada, facilidades na recuperação de desastres e economia de pessoal na operação.

Gerenciamento de TI e Segurança da Informação

A busca de uma solução que ofereça segurança satisfatória a seus usuários é um assunto tão complexo quanto o ambiente tecnológico que o suporta, e as relações entre as entidades que o utilizam. Em decorrência dessa complexidade, torna-se importante observar o ambiente por diversos ângulos. Usualmente, inicia-se resolvendo os aspectos técnicos: a organização lógica da rede, que pode ser centralizada ou distribuída. O ponto de vista administrativo é deixado para uma segunda fase, na maioria das implementações.

A entidade com maior reconhecimento mundial na preparação de profissionais da área de Segurança da Informação é a International Information Systems Security Certification Consortium (ISC), que congrega milhares de profissionais em todos os continentes. Essa entidade condensou em dez áreas de concentração ou "domínios" os diversos conhecimentos que, uma vez aplicados, materializam a Segurança da Informação, de modo a facilitar sua compreensão, estudo e aplicação. Ela chama este cabedal de CBK (Commom Body of Knowlwedge), que pode ser traduzido como "Corpo Comum de Conhecimentos". O profissional aprovado por essa entidade recebe a certificação CISSP® - Certified Information Systems Security Professional.

[2] ACL (access control list): uma lista que descreve regras a serem instaladas em um equipamento.

A necessidade de garantir que a TI entregue valor a seus usuários também é preocupação de outras entidades, como a Information Systems Audit and Control Association (ISACA), que publica o framework Control Objectives for Information and Related Technology (COBIT), cujo enfoque é no sentido da governança, e a Office for Government Commerce (OGC) da Inglaterra, que publica a norma ITIL v3, voltada ao gerenciamento. Essas entidades ocupam-se de aspectos específicos da TI, e ainda que suas normas possuam alguma sobreposição, elas costumam ser utilizadas de maneira complementar, aproveitando-se os pontos de cada uma que melhor se adaptam à organização considerada, obtendo-se assim uma ampla cobertura, que nenhuma das duas oferece sozinha.

Apesar da necessidade de considerar a Segurança Cibernética sob os diversos ângulos apresentados, considera-se neste artigo somente uma das facetas mais sensíveis: a gestão da segurança da informação aliada aos requisitos e técnicas de controle de acesso. Porém, para isso, faz-se necessário explorar o conceito utilizado por todo o cabedal de segurança da informação, que corresponde à tríade da Segurança da Informação, **CID - confidencialidade, integridade e disponibilidade** (Página 4 - Access Control):

- **Confidencialidade:** prevenir o acesso a informações críticas que possuem um determinado rótulo de classificação;
- **Integridade:** impedir mudanças não autorizadas ou modificações impróprias por pessoas autorizadas;
- **Disponibilidade:** garantir que a informação estará disponível para acesso no momento em que um sujeito autorizado desejar ter acesso.

O planejamento de Segurança da Informação

A dificuldade de um Gestor de Segurança da Informação na implantação da segurança cibernética esbarra, na maioria das vezes, na definição do escopo de trabalho (o que realmente deve fazer parte da Arquitetura de Segurança da Informação da organização) e do tipo de controle de acesso que vai permear essa arquitetura. Para clarear esses pontos, o planejamento da Segurança Cibernética tem início com as seguintes tarefas:

Aprovação do Programa de Segurança pela Alta Direção da Organização.

O Programa de Segurança da Informação corresponde a um esforço de diversos setores da organização, principalmente da alta direção, que o institui e mantém, sendo seus objetivos principais:

- Criar uma estrutura lógica que possibilite a implementação de controles;
- Padronizar a estrutura para as diversas plataformas tecnológicas;
- Considerar os diversos tipos de usuários, quer sejam funcionários, clientes ou parceiros;
- Atender aos requisitos legais;
- Criar acesso à informação com Autenticação e Autorização semelhantes em todos os ambientes;
- Planejar a disponibilidade da informação para suportar o ambiente de negócios;
- Ser flexível e adaptar-se às mudanças do ambiente; e
- Ser profundamente comprometido com as necessidades da organização.

Como o nome sugere, o Programa de Segurança da Informação é o esforço para planejar e implementar uma solução de proteção à informação, que atenda às necessidades de toda a organização e que mantenha sua coerência ao passar-se de um a outro departamento, evitando que haja solução de continuidade e falhas de segurança, sendo um importante requisito à interoperabilidade entre sistemas distintos.

A escolha de soluções deve contemplar todo o parque instalado e sistemas disponíveis, sendo que um ponto importante a observar é evitar-se a escolha de uma solução que torne a organização refém de um único fornecedor ou tecnologia, por intermédio da busca por flexibilidade e padrões abertos, sempre que possível.

A norma de referência para esse programa de segurança é a ABNT NBR ISO/IEC 27002:2005,

que tem ampla aceitação no mercado e consolida as melhores práticas em Segurança da Informação, conforme a ISO 27001. Seu objetivo é demonstrar que a segurança cibernética é resultado de um conjunto de ações, com planejamento apoiado pela alta direção da organização, e que sua implantação deve obedecer a critérios técnicos, embora sempre alinhada à visão do negócio.

Para estruturar essa arquitetura de segurança e dar amparo legal às ações subsequentes, é necessário criar um corpo de Políticas, Normas e Procedimentos que suportarão e darão validade legal aos processos de segurança da informação. Isso deve ser iniciado e endossado pela alta direção da organização. Segundo FONTES, 2008, esse corpo de regulamentos deve contemplar os aspectos mais importantes de segurança da informação, buscando pelo menos os seguintes requisitos:

- Proteção do ambiente físico: cuidados a serem observados tanto no controle de pessoas com acesso físico aos computadores e equipamentos de redes, quanto nos cuidados com relação à energia elétrica, ar condicionado e sistemas de proteção contra incêndio.
- Desenvolvimento e implantação de aplicações: para o desenvolvimento interno, é importante que se escolha uma metodologia com ampla aceitação no mercado, evitando assim a dependência de um único grupo ou profissional. Também são importantes a produção e a preservação da documentação (requisitos, projetos, testes de aceitação, documentação de código fonte, etc). Na implantação, é de grande relevância observar rigorosamente os testes de aceite e a fase de migração dos dados. Como estratégia segura, é interessante manter os dois sistemas em paralelo durante algum tempo, pelo menos até que sejam feitas algumas consolidações mensais, por exemplo, para que haja um ponto de controle cujo ciclo seja maior e que possa ser usado como comparação com o sistema anterior.
- Proteção dos recursos de TI: proteção da rede de computadores, pelo emprego de recursos de proteção e detecção de ataques a redes de computadores, tais como firewalls e Intrusion Detection System (IDS)/Intrusion Prevention System (IPS). Proteção individual das máquinas, iniciando pela descoberta e correção de falhas de segurança em sistemas operacionais, por meio de atualizações de segurança, inclusive, se necessário, com atualizações de firmware dos equipamentos dedicados.

Classificação da informação

Definição dos níveis de sigilo da informação e do nível de acesso dos funcionários, principalmente dos Gestores e Custodiantes da informação.

Garantia do acesso à informação

Para garantir a o acesso à informação, é necessário criar regras e mecanismos que protejam a informação, liberando o acesso somente às pessoas autorizadas (e gerando o histórico dos acessos negados/autorizados).

- **Gestão de identidade:** como identificar os usuários e manter atualizados os dados dos usuários autorizados: cadastro, alteração, revogação de acessos, etc;
- **Gestão de autenticação:** verificação da veracidade do usuário e escolha das técnicas de autenticação utilizadas pela organização;
- **Gestão de autorização:** criação de regras de acesso, criação e manutenção de perfis de acesso, verificação de que o usuário possui o perfil necessário para acesso à informação.

Planejamento de contingências

Soluções e procedimentos necessários para as situações que ameacem a sobrevivência da organização, buscando diminuir os impactos e restaurar a capacidade operacional no mais curto prazo.

Garantir a resiliência operacional:

É necessário estabelecer mecanismos que incorporem tratamento das situações adversas ao

cotidiano das operações. Os frameworks de gestão de TI são excelentes modelos para a organização da TI, e o framework ITIL contempla essas necessidades com o processo de Gestão de Problemas, Gestão de Recursos, Gestão de Mudanças e Gestão de Capacidade.

Figura: Programa Corporativo de SI (FONTES, 2008, adaptado pelos autores)

Tratamento dos incidentes de segurança

Em organizações de maior porte, é necessária uma equipe com capacidade técnica e recursos para realizar a detecção de incidentes de segurança, o tratamento inicial, o registro e o encaminhamento para a solução definitiva, que muitas vezes gerará mudanças de procedimentos, tecnologias e processos. Essa equipe é conhecida pela sigla CSIRT (Computer Security Incident Response Team).

Prevenção de fraudes

Os recursos de TI, como a possibilidade de acesso remoto a outros equipamentos, facilidade de copiar informações por meio da rede e de modificar os dados armazenados sem que haja contato físico por parte dos usuários, possibilitam que ocorram fraudes praticamente indetectáveis. É necessário estudar os processos e sistemas em uso para dificultar ao máximo o mau uso dos recursos de TI disponíveis. A atividade de coleta de registros de acesso e auditoria nos processos arquivados é parte fundamental da segurança de TI.

Preservação de evidências de crimes digitais

Para realizar a perícia forense computacional, além dos equipamentos específicos e infraestrutura mínima de coleta de dados, é necessário treinamento específico para que as equipes de TI saibam preservar e coletar indícios de fraudes e crimes digitais. A coleta e preservação é muito dificultada pela volatilidade dos dados, que podem estar presentes apenas em registradores (componentes do processador) ou em memória RAM[3].

Criação de cargos e funções de segurança

Para que seja efetiva, a equipe de segurança deve ser incorporada ao organograma da organização, com funções e escopos de atuação bem delimitados. Se a equipe de segurança não for definida, é comum que as tarefas de segurança acabem sendo relegadas a segundo plano ou mesmo abandonados após certo tempo. Também é desejável que não haja subordinação da equipe de segurança às equipes de operação, pois normalmente ocorrerão conflitos de interesse entre a fiscalização e a execução das tarefas.

Programas de conscientização

Todo o esforço de garantir a segurança é confrontado com o interesse e cultura de seus usuários. É necessário gerenciar a criação de cursos e eventos para treinar e conscientizar os colaboradores. O programa deve ser orientado pelas Políticas de Segurança da organização e pelo ambiente operacional real, fazendo as atualizações de acordo com as mudanças de ambiente, estrutura, tecnologias e ameaças.

A figura a seguir sintetiza os aspectos mais importantes de um programa corporativo de segurança da informação.

4 DESENVOLVIMENTO

Ambiente inicial

A organização objeto deste estudo de caso, aqui denominada XYZ, entidade de direito público, possui algumas características que a diferenciam de suas congêneres de direito privado, tais como a baixa rotatividade de colaboradores, a dependência de políticas públicas e a submissão de seus atos à

[3] RAM (Ramdom Access Memory) é a parte da memória principal onde os programas são carregados e executados. [5]..

fiscalização administrativa por órgãos de controle.

Essa organização provê serviços para vinte e dois clientes internos. Cada um dos quais possuidor de características, público e objetivos distintos. O provedor de serviços e os clientes possuem graus de interdependência variados entre si. Cinco clientes possuem autonomia financeira, orçamento e planejamento próprios, enquanto os restantes são subordinados a um órgão central que controla os orçamentos e coordena as operações.

Na área de Tecnologia da Informação e Comunicações (TIC), a XYZ possui uma Divisão de Tecnologia da Informação (DTI), que presta suporte à matriz e coordena algumas atividades das filiais. Porém, cada filial conta com sua própria equipe de suporte técnico e realiza seus controles de acesso de forma independente, exceto algumas atividades de TIC que envolvem mais de uma filial e que são coordenadas pela DTI.

Nesse ambiente departamentalizado, em que cada organização possui objetivos e públicos diferentes da outra, estabeleceram-se ambientes independentes e fechados, à semelhança de pequenos "feudos", no qual as regras e grau de controle dependiam quase que exclusivamente da capacidade e interesse da equipe local.

A automatização dos sistemas administrativos e de controle modificou os processos organizacionais, pois a informação, que circulava por via de documentos impressos, passou a ser produzida digitalmente e distribuída por meio eletrônico. Para facilitar a administração dos sistemas e circulação da informação, a hospedagem dos sistemas informatizados foi centralizada na matriz e estabeleceram-se enlaces de redes com as filiais.

Nesse novo cenário, com toda a organização interconectada, os efeitos de incidentes de segurança, em qualquer um dos muitos equipamentos, passaram a afetar toda a rede. Por exemplo, a contaminação de um equipamento pelo vírus residente no pendrive pessoal de um colaborador, agora afetava a todos os computadores da organização, pois a conectividade é explorada pelos agentes maliciosos para se disseminar rapidamente por todo o sistema.

Planejamento da Solução

Gestão de Segurança da Informação

A vulnerabilidade da rede de computadores da organização, que passou de uma situação de pontos isolados para uma rede totalmente interconectada, gerou a necessidade de que a DTI identificasse os novos requisitos de segurança. Notícias constantemente veiculadas pela mídia divulgam que grandes empresas e governos são alvos frequentes de ataques de grupos de hackers, gerando muitas vezes graves prejuízos financeiros, perda de informações privadas de clientes e consequente perda de confiança na organização.

Constatou-se que a descentralização ainda existia em alguns pontos, remanescente da situação de isolamento anterior, juntamente com a falta de procedimentos padronizados e que tais fatos poderiam propiciar falhas graves de segurança. Para vencer as resistências às práticas de segurança, a DTI valeu-se de notícias divulgadas sobre os sucessos de grupos hackers para sensibilizar a diretoria da XYZ no sentido de iniciar um programa corporativo de segurança da informação, buscando difundir e aplicar as melhores práticas, harmonizar as tecnologias utilizadas e padronizar soluções entre as filiais.

A Comissão de Segurança da Informação (CSI)

A primeira providência da DTI foi obter a aprovação da diretoria para estabelecer uma comissão de gestão de segurança da informação (CSI), a fim de estabelecer objetivos e definir o escopo de atuação.

Houve a tentativa inicial de envolver gerentes de outras áreas da organização no trabalho de listar objetivos e requisitos de segurança da informação, devido ao conhecimento que cada um possuía sobre sua área de atuação, porém sem sucesso, pois culturalmente o termo "segurança da informação" era percebido como sendo atribuição exclusiva da DTI, de forma que a comissão foi composta por técnicos e pelo Diretor de TI, não se conseguindo incluir usuários na equipe.

Seguindo as recomendações da norma ABNT NBR ISO/IEC 27002:2005 (págs 'x',8,24,29,108-111), que trata de práticas para a segurança da informação, a comissão definiu os seguintes

controles como prioritários, tendo como base seu conhecimento inicial da situação da organização:

- proteção de dados e privacidade de informações pessoais: o direito à privacidade, protegido pela Constituição Federal em seu artigo 5º, impõe às organizações que protejam os dados pessoais e a privacidade de informações pessoais de seus funcionários, clientes, fornecedores e associados de qualquer natureza, que possuam registros sob responsabilidade da organização.
- proteção de registros organizacionais: é necessário definir normas para retenção, armazenamento, tratamento e disposição de registros, manter um inventário das fontes de informação mais importantes e implementar controles apropriados que os protejam de perdas, falsificação e destruição;
- documento de Política de Segurança da Informação: define a segurança da informação, seus princípios, metas e escopo, e a estrutura do gerenciamento de risco; alinha os princípios de segurança com os objetivos organizacionais, legislação, normas e contratos vigentes; define responsabilidades gerais e específicas, as consequências das violações da política de segurança e serve claramente como marco da política geral da organização, a qual todos os indivíduos e organizações que se relacionam com a mesma devem conhecer e respeitar.
- gestão de vulnerabilidades técnicas: quando as vulnerabilidades técnicas, tais como falhas de implementação, bugs e erros conhecidos em aplicações e sistemas operacionais são divulgados, inicia-se uma corrida: os fabricantes e usuários buscam a correção ou mitigação e os hackers tentam aproveitar-se desaa fraqueza para desferir ataques cibernéticos. É necessária a criação de procedimentos de teste, correção e entrega de novas versões, bem como a manutenção de uma base de informações e pessoal capacitado para aplicar as correções ou medidas, a fim de mitigar os riscos.
- gestão de incidentes de segurança da informação e melhorias: é necessário definir responsabilidades e procedimentos que garantam o monitoramento, a avaliação e a gestão dos incidentes de segurança. Alguns casos exigem a realização de testes específicos e em outros, quando se suspeita de violações da política de segurança ou mesmo da ocorrência de crimes, torna-se necessário realizar a perícia forense em computadores e equipamentos de TI. Após avaliação dos danos causados e da causa-raiz, é importante incorporar às rotinas de proteção as lições aprendidas com o incidente, aplicando mudanças corretivas no ambiente.

Diagnóstico da situação inicial

O próximo trabalho da CSI foi realizar um diagnóstico de situação da matriz e filiais, obtendo um inventário da infraestrutura, equipamentos, enlaces de rede e pessoal.

Concluído o levantamento, ficou claro para a CSI que a maior ameaça existente à segurança era a "porosidade" da rede, ou seja, o grande número de conexões existentes. Todas as filiais possuíam acesso à Internet, sendo que algumas possuíam mais de um link de acesso. As proteções instaladas não se mostraram adequadas em nenhuma das filiais e nem mesmo na matriz. A existência de diversos acessos à Internet, com baixo controle e parcos recursos de segurança, permitiria facilmente a evasão de dados da organização e a invasão por hackers.

A inexistência de controles adequados nas filiais, bem como a falta de registros dos acessos, colaboraram no sentido de definir como prioritária a melhoria da interligação entre as redes da matriz e das filiais e a centralização do acesso à Internet, estabelecendo que as filiais iriam acessar a Rede Mundial unicamente por meio da matriz, resultando então em uma rede mais protegida e segura, com um único ponto de acesso à Internet.

A capacitação do pessoal, tanto da matriz quanto das filiais, observada no relatório, comprovou a falta de conhecimentos específicos na área de segurança da informação em toda a organização, gerando a necessidade de um plano de capacitação que

suprisse as necessidades atuais e futuras de profissionais especializados.

O levantamento realizado permitiu o planejamento das ações a serem empreendidas, gerando quatro produtos:

- **Plano de Gerenciamento de TI:** para atender plenamente os controles recomendados pela norma ABNT NBR ISO/IEC 27002:2005 optou-se em aderir aos padrões da indústria, tais como ITIL e COBIT, ainda que esse processo leve um tempo maior de implementação.
- **Plano de Capacitação de Pessoal:** definição de perfil técnico do pessoal de TI e contratação de cursos para capacitação que permitam implantar a segurança imediatamente, e o gerenciamento em uma segunda fase.
- **Projeto de Atualização das Normas de Segurança** da organização, unificando as diversas regras existentes na matriz e nas filiais e publicando a Política de Segurança da Informação e Comunicações (PoSIC).
- **Projeto Centralização de Internet (PCI):** para melhoria imediata da interligação matriz-filiais e contratação do link centralizado de acesso à Internet com a infraestrutura necessária.

Plano de Gerenciamento de TI

Ao realizar o estudo da situação da TI na organização, ficou evidente a necessidade de um planejamento que considerasse o melhor emprego dos recursos financeiros, a necessidade de padronização de tecnologias e maior controle da TI.

A necessidade de oferecer melhor suporte ao negócio, diminuição de tempos de atendimento e aumento da capacidade de disponibilidade da TI é endereçado pelos frameworks de gestão de TI, como o ITIL v3 e o COBIT 5, cujo foco é justamente gerência de serviços e governança de TI, respectivamente.

Integrando o gerenciamento, foi criado um calendário de visitas técnicas da DTI às filiais, nas quais foram verificados os dados existentes e as condições da infraestrutura, equipamentos e procedimentos de trabalho, bem como realizados ajustes e configurações de equipamentos.

Plano de Capacitação de Pessoal

Para que fossem implantados os controles definidos previamente, tornou-se necessária a capacitação das equipes de TI. O planejamento de capacitação considerou ser importante concentrar esforços na equipe que seria responsável por garantir a segurança da informação, uma vez que essa deveria manter a disponibilidade do único acesso à Internet doravante disponível, sob pena de isolar a instituição.

Visando facilitar o treinamento e tornar mais efetivo o emprego dos profissionais, foram definidas duas linhas de preparação do pessoal:

- **Linha Gerencial:** capacitando ao estudo, análise e planejamento atual e futuro pelos analistas e chefes de equipe;
- **Linha Operacional:** capacitando os técnicos e analistas para o emprego imediato na segurança da rede.

A capacitação da equipe de TI para atingir os objetivos levantados contemplou os cursos a seguir listados, escolhidos após consulta das ementas e levantamento de informações com profissionais possuidores dos cursos sobre a real necessidade e utilização dos conhecimentos na proteção da rede de computadores:

Linha Gerencial, com cursos nos níveis técnico e gerencial:

- ITIL Foundations, para toda a equipe: o framework ITIL v3 é reconhecido mundialmente como sendo as melhores práticas de gestão para serviços de TI.
- Auditor Lider de segurança da Informação - ISO 27001, para toda a equipe, pela necessidade de vistoriar e orientar os trabalhos das filiais, bem como gerar relatórios e procedimentos para toda a organização e ministrar capacitação e conscientização aos demais funcionários.
- COBIT, para os analistas: a organização que supervisiona e mantém financeiramente a XYZ tem entre seus objetivos estratégicos

a governança. O framework COBIT é adequado ao objetivo da mantenedora ao trabalhar com Governança de TI e complementa os planejamentos já realizados com ITIL.

- Preparatório para certificação CISSP, para os analistas: a certificação CISSP é a mais reconhecida na área de segurança da informação pelos próprios profissionais, pela preparação em nível gerencial e pela abrangência de assuntos abordados, a qual se divide didaticamente a Segurança da Informação em dez (10) áreas temáticas.

Linha Operacional, com cursos nas áreas de segurança de redes:

- Segurança da Informação - Conscientização e Treinamento: capacitação de funcionários na aplicação da PoSIC. Curso interno, ministrado pelos integrantes da CSIRT.
- Gerenciamento de Incidentes (Básico e Avançado) - CERT.br[4], para os técnicos que manterão a infraestrutura de acesso e os principais servidores da organização.
- Hacker Ético, para os analistas de rede que comporão o grupo de gerenciamento de incidentes e que realizarão os testes de penetração na rede da empresa e de filiais, localizando e fechando brechas na segurança de perímetro, de servidores e serviços.
- Perícia Forense Computacional, para os analistas encarregados de localizar e interpretar vestígios de crimes digitais nos computadores e equipamentos de TI da organização.

Política de Segurança da Informação e Comunicações (PoSIC)

Segundo a ABNT NBR ISO/IEC 27002, a Política de Segurança da Informação deve "prover uma orientação e apoio da direção para Segurança da Informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes".

Por meio desse documento será demonstrado o comprometimento da alta direção com a segurança, serão definidas as diretrizes gerais de segurança da informação e garantida à implementação dos controles necessários. O documento deverá definir responsabilidades gerais e específicas e auxiliará inclusive na seleção de produtos e no desenvolvimento de processos e de documentos.

A CSI revisou e organizou as normas existentes em um único documento, que foi atualizado com as recomendações da norma ABNT NBR ISO/IEC 27002:2005, gerando uma "Política de Segurança da Informação e Comunicações" e um "Termo de Uso dos Recursos de TI", documentos que deverão ser divulgados a toda organização. O "Termo de Uso" deverá ser assinado por todos os usuários antes da utilização do novo acesso à Internet e pelos novos funcionários quando forem admitidos na organização.

Projeto Centralização de Internet (PCI)

O levantamento inicial permitiu identificar os fatores de maior impacto na segurança da rede, já considerando que a centralização do acesso iria causar um efeito colateral muito ruim. Ao concentrar diversas filiais em um único link de acesso, este ganha visibilidade e se transforma em um alvo compensador, pois as chances de um ataque direcionado obter sucesso é proporcional à quantidade de máquinas-alvo, exposição e possíveis vulnerabilidades que o alvo oferece.

Preventivamente a essa hipótese, foi planejada uma configuração de equipamentos de maior capacidade e especialização para a proteção desse link, implementando a defesa em profundidade, conforme ilustra a figura 2, agregando a partir da borda da rede equipamentos e configurações que acrescentam, sucessivamente, maior proteção à rede.

Uma das táticas utilizadas foi a utilização de firewalls de diferentes fabricantes e sistemas operacionais na borda e na rede interna para dificultar a ação de hackers, pois mesmo que um

[4] O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) é mantido pelo NIC.br, do Comitê Gestor da Internet no Brasil, e atende a qualquer rede brasileira conectada à Internet.

firewall possua alguma vulnerabilidade que seja explorada, provavelmente o outro equipamento não estará sujeito ao mesmo tipo de ataque cibernético.

Na organização representada na figura 2, a seguir, os retângulos de tom mais claro indicam uma área com menor controle, enquanto os de tom de mais escuro uma localidade com maior proteção lógica. O datacenter já é uma fração mais protegida da organização, a sala de servidores um setor mais restrito do datacenter e, finalmente, um armário "rack" que contém um segmento da rede com nível máximo de proteção. A interligação da rede externa com a interna atravessa uma sequência de equipamentos que realizam a análise e filtragem cada vez mais severas: quanto mais sensível a informação, maior será a quantidade de equipamentos e filtros a serem atravessados.

Foram incluídos os equipamentos abaixo, listados para proteção e registro de acessos:

- **Firewall de borda (cluster):** conjunto de firewalls em cluster, que faz a primeira proteção e filtragem dos acessos e tentativa de ataques à rede vindas da Internet.
- **IPS (Intrusion Prevention System):** logo após o firewall, o IPS verifica as conexões e inspeciona os pacotes de rede pelo seu conteúdo. O IPS atua no nível de Aplicação, considerando o modelo TCP/IP.
- **Switch Core com módulo de firewall:** possui capacidade de roteamento e de filtragem de pacotes, atuando tanto como roteador como firewall, segmentando o conjunto de máquinas em redes distintas, de forma a isolar o tráfego de segmentos e filtrar por critérios definidos pelo administrador da rede o tráfego de um para outro segmento da rede.
- **Proxy hierárquico:** realiza o cache de conteúdo acessado na Internet e distribui aos proxies instalados nas filiais.
- **Proxy Reverso:** faz cache das páginas internas acessadas pelos clientes externos, acelerando as consultas e diminuindo a carga de trabalho e o risco de ataques aos servidores internos.

Gestão de vulnerabilidades técnicas

Infraestrutura de hospedagem do site principal

O fornecimento de energia era um fator de risco, pois a sala de servidores existente na matriz, apesar de contar com gerador e UPS, não possuía alimentação corretamente dimensionada e a energia que alimentava o datacenter e os condicionadores de ar estava distribuída a partir de um único quadro, que inclusive alimentava todo o andar do edifício.

Foi necessário criar um quadro de energia específico para o datacenter, alimentado com duas fases e instalar cada equipamento de ar-condicionado em uma das fases de energia diferentes, de forma que mesmo que aconteçam quedas em uma das fases, a outra linha de energia poderá suportar 50% da carga de ar-condicionado, suficiente para manter a sala refrigerada por um período de cerca de 2 horas.

O aterramento elétrico também foi refeito, de forma a atender com segurança os equipamentos do datacenter.

Segmentação das Redes e regras de firewall

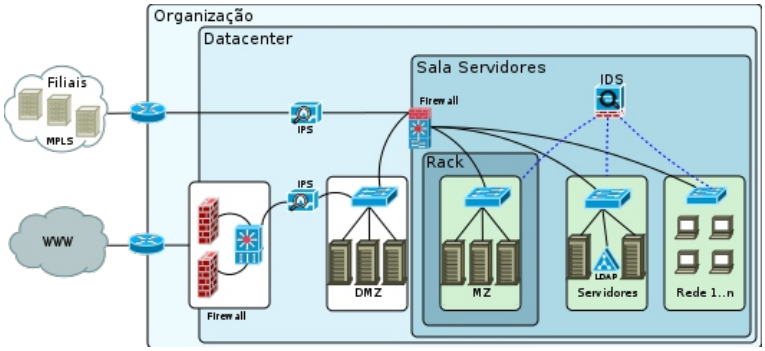


Figura: Diagrama exemplo de defesa em profundidade.
Fonte: dos autores.

Foi realizada a segmentação das redes, criando-se subredes para cada filial e para segmentos do datacenter. No datacenter foram implementadas as redes abaixo listadas, e o acesso de uma rede a outra somente é liberado por meio de regras nos firewalls.

- DMZ: Zona Desmilitarizada, que compreende os serviços que devem ser acessados pelo público em geral, conexões originadas na Internet.
- MZ: segmento de rede mais protegido, com

bases de dados e arquivos de uso restrito de algumas aplicações e usuários.

- Servidores de uso interno.
- Rede de Gerência, utilizada pelos técnicos que administram os servidores e pelos equipamentos NAS[5] de backup primário (os dados são gravados em fita em um segundo momento).
- Rede das filiais, interligadas por meio de tecnologia MPLS que segue um plano de numeração centralizado pela DTI. Essa tecnologia permite o tráfego de dados, voz e vídeo, gerando facilidades adicionais e economia de recursos, uma vez que reduz os custos com tarifas de telefone e permite as videoconferências, economizando tempo, dinheiro e deslocamentos de pessoal.

A política padrão estabelecida para os firewalls é **bloquear**, sendo que a inclusão ou alteração de regras deve ser solicitada por Ordem de Serviço e implantada somente depois de analisada e documentada pela equipe de segurança (CSIRT), que possui autonomia para não aprovar regras que violem a segurança definida para cada segmento de rede.

Servidores

Houve uma constatação preocupante com relação aos servidores. Apesar de existirem em quantidade suficiente para hospedar os sistemas e aplicações necessários, não havia ambiente de homologação para testar as correções e patches, podendo gerar panes inesperadas por uma simples atualização do sistema operacional.

A DTI passou a implementar seus servidores utilizando software de virtualização, que apresenta diversas vantagens operacionais, sendo a mais importante, nesse caso, a capacidade de copiar uma máquina virtual em produção para a execução de testes de homologação com dados reais.

Gerenciamento de Identidade

A escolha do sistema de gerenciamento foi pelo modelo descentralizado, uma vez que as filiais possuem autonomia para contratar e demitir funcionários, ficando encarregadas de atualizar a lista de usuários.

A solução implementada foi baseada no serviço de diretórios opensource OpenLDAP, que permite criar uma árvore central com diversos ramos, na qual cada ramo representa uma filial. O servidor da matriz implementa a raiz da árvore, e cada filial é responsável pelo cadastro/alteração/exclusão de seus funcionários. Os cadastros assim realizados permitem que os funcionários possam acessar diversos recursos de TI de qualquer filial, pois o serviço de diretórios, além do armazenamento centralizado, permite a replicação da base de dados pelas filiais, para utilização pelos serviços locais, que contará então com a base de dados atualizada de todos os funcionários da organização.

Gerenciamento de Acesso

No projeto PCI, o acesso à Internet é condicionado ao uso de identificação do usuário, realizado por meio de "usuário e senha", que serão checados antes do acesso ser concedido.

O perfil do usuário para acesso a internet é armazenado no proxy central, que possui 2 perfis:

- acesso **normal**: acesso a todos os sites da Internet, desde que não bloqueados pela gerência de redes.
- acesso **VIP**: acesso irrestrito a qualquer site da Internet.

Independente do perfil do usuário ser "acesso normal" ou "acesso VIP", todos os registros de acessos são gravados e também salvos em banco de dados para consultas posteriores. O perfil de consumo diário de cada filial é gerado e disponibilizado à CSIRT, que acompanha para monitorar anomalias na rede.

Os registros foram centralizados no site central por que esse possui mais estrutura de armazenamento, de contingência e controla rigidamente o acesso aos logs, evitando modificações ou exclusões de registros, fato que

[5] NAS: Network Attached Storage - servidor de arquivos que oferece basicamente espaço em disco para outros computadores, por meio de rede TCP/IP, emulando de comandos de acesso à disco (camada 3 da arquitetura SCSI) nos pacotes de rede[6]

poderia acontecer em filiais até mesmo pela falta de conhecimento dos técnicos. Outro determinante é o fato de que o contrato com a operadora de telecomunicações foi firmado pela matriz, de forma que a responsabilidade, para fins jurídicos, é dessa localidade.

Semanalmente, cada setor de TI das filiais recebe um relatório de consumo (em bytes) discriminado por usuário. Para acompanhamento mais próximo, a equipe de cada filial pode acessar os relatórios diários de acesso de quaisquer usuários sob sua responsabilidade.

Proxies hierárquicos

Os proxies do PCI são o *proxy* central e os proxies das filiais, em formato de árvore invertida. Os acessos iniciados em qualquer filial são armazenados no proxy central que mantém os dados em memória/disco durante algum tempo. Quando existe outra requisição do mesmo dado/documento, não há a necessidade de carregar novamente o mesmo dado do site original, bastando enviar o já armazenado.

Melhorias implementadas ao final do Projeto PCI

Ao terminar de implantar o PCI, o ambiente (em geral) de TI já havia se alterado bastante, pois as mudanças introduzidas no ambiente inicial, sejam para viabilizar o projeto, ou por consequência desse, extrapolaram o previsto inicialmente, de forma que algumas mudanças eram diretamente relacionadas ao projeto e diversas outras interfaceavam com mudanças da infraestrutura e, principalmente, mudanças de gestão da TI.

Foram modificados os serviços ofertados, processos, infraestrutura, documentos e serviços a seguir listados:

- Criação de uma Política de Segurança da Informação e Comunicações em um Termo de Uso dos Recursos de TI, aplicada a toda a organização;
- Centralização do gerenciamento de Identidade, possibilitando a identificação de um funcionário em qualquer ponto da rede e uso dessa identificação nos diversos serviços ofertados;
- Centralização do acesso à Internet, com ferramenta de acompanhamento dos registros de acesso que fornece relatórios gerenciais;
- Centralização de servidores de e-mail: todos os serviços de e-mail da XYZ foram centralizados em um único servidor multi-domínios, que além de oferecer proteção pelos controles instalados, também evita que informações e documentos internos circulem por servidores públicos da Internet;
- Oferta de um serviço de chat interno, usando o serviço de Identidade centralizado, e facilitando a comunicação interna entre todos os funcionários e todas as filiais;
- Centralização da hospedagem de websites em um ambiente seguro;
- Novos serviços de monitoramento da rede e inventário do parque instalado (MONIM, OCSInventory, ZABBIX, NAGIOS) que permitem obter relatórios e dados sobre os incidentes, melhorando a capacidade de decisão e ação das equipes;
- Oferta de espaço de backup remoto às filiais;
- Melhorias na infraestrutura de TIC da matriz e das apoiadas;
- Constituição e treinamento da CSIRT, diretamente subordinada à Presidência, que realiza a análise de vulnerabilidades de servidores e aplicações antes da entrada em produção e monitora o uso da rede;
- Aquisição e instalação de equipamentos e softwares dedicados à proteção de rede e perícia forense computacional;
- Implantação das visitas de Auditoria de Segurança da Informação, que abrangem todas a filiais, com calendário divulgado anualmente;
- Instituição do Plano de Capacitação de Pessoal, revisado anualmente.

Fatos Gerenciais Observados

Ao implantar o projeto PCI, diferente da expectativa inicial da DTI, a maior dificuldade não foi a liberação de orçamento para o projeto, que ocorreu de forma natural após a percepção pela Diretoria da importância e da premência de melhorar a segurança da organização. A maior dificuldade percebida foi gerenciar e executar as mudanças a serem implantadas em filiais que possuíam orçamento próprio e maior autonomia que, via de regra, acabavam por reclamar da ingerência "externa" em assuntos que consideravam de sua esfera de decisão. Em casos assim, as reclamações geralmente não continham elementos técnicos, tais como indicadores, registros e dados coletados, que embasassem tecnicamente o problema reportado, mas apenas relatos de insatisfação com o serviço, de forma genérica e imprecisa.

CONCLUSÃO

Devido à aprovação e comprometimento dos diretores, foi implementada uma Política de Segurança da Informação em conformidade com as principais normas de segurança da informação, que foi divulgada e aplicada rigidamente para toda a instituição. Este marco inicial possibilitou as demais mudanças.

O acesso à Internet na empresa XYZ passou a ser realizado unicamente por meio da matriz. A implantação de controles na borda da rede e constituição de uma equipe de segurança, permitiu a aplicação da PoSIC.

O gerenciamento centralizado de Identidade permitiu ofertar soluções antes inexistentes nas filiais, tais como permitir que um funcionário de uma filial acessasse seus recursos estando em outra, e conexões VPN aos funcionários em trânsito, possibilitando o acesso permanente à informação necessária.

A centralização dos servidores de e-mail e o serviço de chat corporativo foram bastante elogiados pelos usuários, pela rapidez no tráfego dos e-mails internos e a facilidade de troca de informações proporcionada pelo chat, bem como a melhoria da infraestrutura de acesso, segurança e hospedagem.

A implantação dos sistemas de monitoramento centralizado permitiu obter dados e relatórios sobre os incidentes de rede que raramente eram percebidos pelos administradores, haja vista as administrações descentralizadas, o que caracterizava uma falta de padrão e informações não contabilizadas e com excesso de privilégios. Cabe ressaltar a melhor capacidade de operação e decisão da equipe, bem como o embasamento claro e preciso das solicitações para a liberação de orçamento para investimento e capacitação, por ocasião dos planejamentos anuais.

O Plano de Capacitação, ainda em fase de execução, já propiciou o treinamento de toda a equipe com pelo menos uma capacitação por funcionário da gerência de redes e da equipe de segurança, possibilitando desde seu início que a equipe já pudesse iniciar a implantação dos controles previstos.

Embora ainda existam trabalhos em andamento na área de infraestrutura, equipamentos de segurança, processos internos e capacitação, a avaliação da Presidência da XYZ e da DTI é de que houve significativa melhoria na oferta de serviços, na gerência da rede e nos controles de segurança. Essa percepção tem sido corroborada nas visitas técnicas da DTI às filiais e nos contatos com os usuários.

As técnicas e passos adotados podem ser adaptados a outras organizações que desejem implantar práticas de segurança da informação.

REFERÊNCIAS

ZWICHY, E. D.; COOPER, S; CHAPMAN, D. B. **Construindo firewalls para a internet**. 2. ed. Rio de Janeiro: Campus, 2000.

TANENBAUM, A. S. **Redes de computadores**. 4. ed. Rio de Janeiro: Campus, 2003

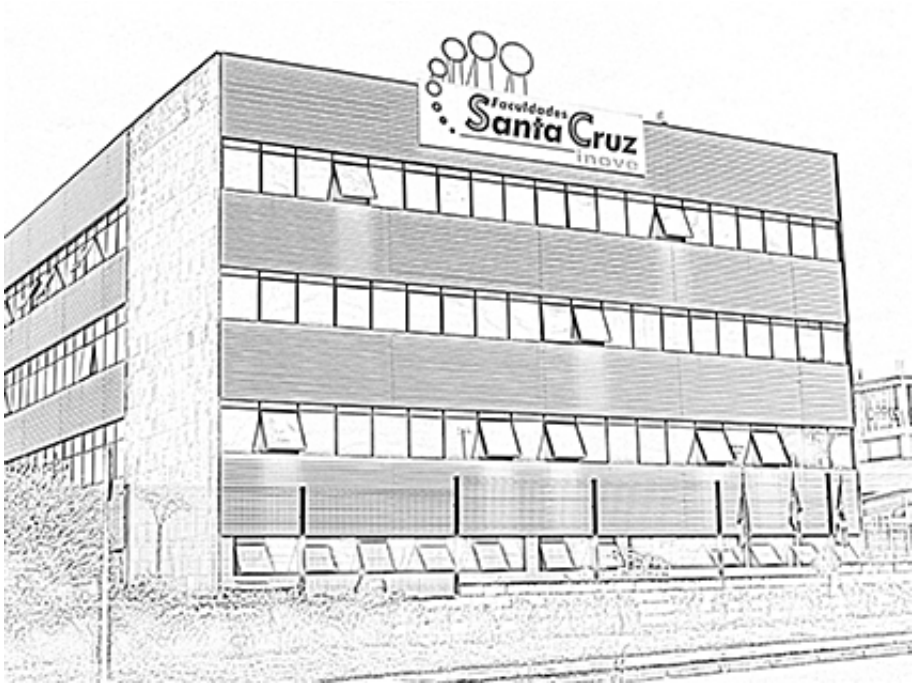
VMWARE - Conceitos básicos da virtualização. Disponível em: <http://www.vmware.com/br/virtualization/virtualization-basics/what-is-virtualization.html>, Acesso em: 28 fev. 2013.

FONTES, E. L. G. Praticando a segurança da informação, Rio de Janeiro: Brasport, 2008.

F. Harold Tipton, "Official (ISC)2 Guide to the CISSP", 2nd Edition, Domain Access Control, 2010, pp. 2-154.

FLYNN, I. M. **Introdução aos sistemas operacionais,** Cengage Learning Editores, 2002.

Linda Null, Julia Lobbur - **Princípios básicos de arquitetura e organização de computadores**, Rio de Janeiro: Bookman, 2010.


Faculdades
Santa Cruz
inove