SEGREGAÇÃO DAS REDES DE TI E TA DA V&M DO BRASIL [1]

Ana Alda Gomes Tavares [2]
Leandro Pfleger Aguiar [3]
Raphael Gomes Pereira [4]

RESUMO
A segregação dos ambientes de rede TA e TI é um dos primeiros passos para a criação de uma estrutura de TA com controles independentes, capazes de atender aos requisitos de segurança mais adequados à área de Automação. Este trabalho tem por objetivo demonstrar o projeto de segregação das redes TI e TA desenvolvido na V&M do Brasil, apresentando as soluções adotadas, os riscos, as dificuldades de implementação e lições aprendidas durante a execução do projeto.
Palavras-chave: Segurança da informação; Tecnologia da informação (TI); Automação (TA); Segregação.

V&M DO BRASIL IT AND AUTOMATION NETWORK SEGREGATION

Abstract
The network segregation of IT and Automation environments is the first step towards building a network infrastructure with segregated controls ready to attend V&M Automation area security and business requirements. This work will demonstrate the IT and Automation networks segregation project executed into V&M do Brasil corporation, addressing solutions, risks, concerns and lessons learned during the project execution.
Key words: Information security**;** Information technology (IT); Automation; Segregation.

[1] *Contribuição técnica ao XI Seminário de Automação de Processos, 3 a 5 de outubro, Porto Alegre-RS*
[2] *Analista de Sistemas, analista de automação da V&M do Brasil.*
[3] *Analista de Sistemas, analista de sistemas da Chemtech.*
[4] *MBA, consultor da Chemtech.*

INTRODUÇÃO

As áreas de Tecnologia da Informação (TI) experimentam hoje um auge tecnológico altamente produtivo. Sistemas de voz sobre IP (VOIP), ferramentas para trabalho cooperativo distribuído (CSCW *Computer Supported Cooperative Work*) e redes móveis (*Wireless*) são exemplos de recursos tecnológicos que trazem às redes corporativas simplicidade nas tarefas, agilidade no trabalho e alta produtividade. Tanta conectividade e mobilidade, apesar de trazerem uma série de benefícios, carregam também a crescente problemática da Segurança da Informação. Com o aumento do uso e confiabilidade nos sistemas computacionais, surge, paralelamente, a necessidade de investimento em mecanismos de proteção que tragam às atividades de trabalho suportado pelo computador a segurança antes tangível através de proteções físicas da informação.

Embora a indústria da automação (TA) não acompanhe com veemência os avanços tecnológicos que surgem constantemente para o ambiente de TI, o desenvolvimento e popularização dos padrões Ethernet e TCP/IP e a forte adoção destes padrões na automação faz com que estas necessidades de segurança tornem-se igualmente indispensáveis no ambiente industrial. Com a utilização do sistema operacional Windows fortificando-se cada vez mais neste ambiente, substituindo até mesmo sistemas operacionais de tempo real, surgem as preocupações com vírus, cavalos de tróia e demais riscos associados a código malicioso e cuja freqüência neste sistema se acentua.

A aplicação de contramedidas de segurança na TI e TA, no entanto, como forma de mitigação de riscos, não pode ser realizada de maneira homogênea, tratando-se estes ambientes de maneira igualitária e com o mesmo rigor. Sistemas de automação são, naturalmente, mais sensíveis a interferências e menos toleráveis a restrições. Da mesma forma, sistemas de TI são mais dinâmicos e, por sua maior suscetibilidade a outros tipos de riscos, devem ser tratados com controles próprios e políticas adequadas às aplicações corporativas. Tal situação torna-se um impeditivo em organizações que tratam os sistemas tecnológicos de automação com as mesmas práticas de segurança.

O Projeto de Separação das Redes da V&M do Brasil surgiu após a identificação desta sobreposição no tratamento e gestão dos ativos de tecnologia da informação para TI e TA, sendo concebido com o objetivo maior de realizar a separação física e lógica destas duas redes. Isto permite a implementação de controles de segurança adequados ao ambiente industrial, com procedimentos específicos e a autonomia exigida pelas diversas áreas de automação, ao mesmo tempo em que exime os gestores de TI de cuidados cuja especialidade não pode ser cobrada. Além deste objetivo, o projeto também endereça a necessidade de atualização tecnológica da TA em termos de arquitetura de rede e implementa controles adicionais para a garantia da organização e segurança, preparando-a para a conformidade com possíveis regulamentações como a ANSI/ISA 99.

Automação na V&M do Brasil

O modelo de gestão da automação da V&M do Brasil torna cada uma das áreas de produção independentes entre si e independentes, em termos, também da Superintendência de Tecnologia da Informação, órgão responsável pelos sistemas de informação da V&M. A manutenção dos sistemas de supervisão é exercida pela gerência de manutenção de cada área de produção. Entretanto, há a figura do

Comitê de Automação (COMAUT), sob a responsabilidade da Engenharia de Automação, órgão gestor centralizado, responsável por definir políticas, estratégias e melhores práticas de automação na empresa.

A manutenção descentralizada garante agilidade na tomada de decisão e flexibilidade para a adoção das melhores soluções. Tanta independência, por outro lado, trouxe o inconveniente da falta de padronização dos ambientes de automação, criando situações em que a hierarquização em níveis de informação não é adequadamente respeitada.

Utilizando a norma ANSI/ISA S95 como referência, pode-se dividir os sistemas existentes na empresa em 5 níveis (Figura 1).

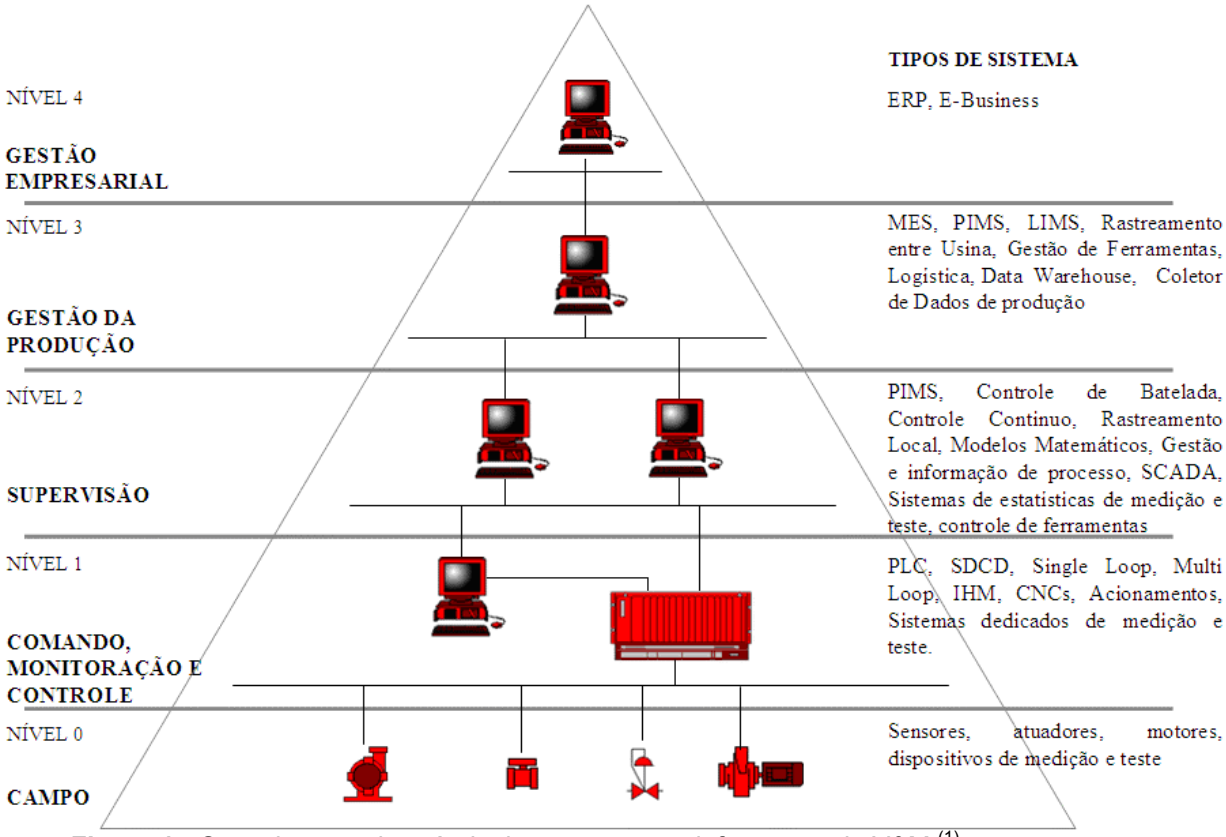

Figura 1 - Conceituação dos níveis de automação e informação da V&M.[1]

Enquanto em algumas áreas de produção há conformidade com este modelo, podendo-se perceber claramente a presença dos cinco níveis, em outras, no entanto, é possível encontrar apenas dois (geralmente os níveis de campo e de controle) ocorrendo uma mistura nos níveis da topologia. Dentre as situações mais críticas resultantes, têm-se equipamentos de TA e TI misturando-se nas arquiteturas física e lógica, com estações de supervisão ou switches de automação conectados a switches da rede corporativa e, portanto, tendo sua disponibilidade, desempenho e segurança vinculados à infra-estrutura da rede corporativa.

Diferenças Entre a TI e TA

Apesar da crescente convergência do ambiente de TA no uso de tecnologias antes características de TI, há diferenças importantes entre estes dois tipos de ambientes que os impedem de serem tratados da mesma forma:

- Volume de tráfego: enquanto na TI as aplicações se caracterizam pelo grande volume de tráfego de dados, justificado pelo uso de aplicações multimídia e internet, na TA normalmente o volume de dados é, comparativamente, pequeno;
- Largura de banda: no ambiente de TA, largura de banda se torna um fator crítico. O volume de tráfego é relativamente pequeno se comparado ao da TI, porém é de extrema importância que se mantenha a qualidade do serviço necessária a aplicações de tempo real. Como exemplo, no ambiente automação o download periódico de atualizações de software poderia comprometer o bom desempenho da rede, prejudicando a comunicação entre dispositivos e aplicações de tempo real, mas, para o ambiente corporativo, não traria grandes problemas;
- Dinamismo: o ambiente de TI, de maneira geral, pode ser visto como flexível e dinâmico, suportando mudanças com facilidade e baixo impacto para o negócio. Na TA operam aplicações altamente sensíveis a paradas, com impactos diretos em resultados em termos de produtividade, tratando-se de um ambiente, portanto, pouco receptivo às mudanças;
- Criticidade das aplicações: aplicações de TI normalmente não se relacionam com processos de produção, nos quais minutos de indisponibilidade possuem um impacto elevado. O custo de tal inoperância é, comparativamente, pouco significativo;
- Nível de acesso: os níveis de permissão para acesso aos sistemas são muito diferentes, existindo exigências de autenticação e autorização específicas que só se aplicam especificamente a cada área.

Estas são as diferenças típicas entre os dois ambientes que criam, como conseqüência, impeditivos críticos que dificultam a concepção de controles de segurança compartilhados entre as áreas.

Ao definir a estratégia de segurança para os ambientes de TI e TA, é essencial levar em conta as diferenças, definindo-se quais os aspectos de segurança devem ser priorizados em cada um dos ambientes. A segurança da informação baseia-se, tipicamente, em três pilares: a confidencialidade, integridade e disponibilidade. No ambiente corporativo, o aspecto mais importante é a confidencialidade, onde somente quem tiver a devida permissão deve ter acesso à informação. Em seguida vêm integridade (garantir que a informação recebida é igual à enviada pelo proprietário) e disponibilidade (garantir que a informação esteja disponível sempre que necessário).

No ambiente de automação, as prioridades se invertem, e o aspecto mais importante passa a ser a disponibilidade, tendo em vista que os sistemas de informação utilizados naquele ambiente estão ligados a processos físicos, e que apenas poucos segundos de indisponibilidade de alguma informação serão suficientes para causar grandes prejuízos. Integridade e confidencialidade vêm em seguida.

Leis e Normas

O processo de gestão do ambiente de TI tem utilizado alguns padrões formalmente estabelecidos, como por exemplo, a ISO/IEC 20000(Gestão de entrega de serviços baseada no ITIL), BS25999 (Continuidade de negócios) e por último a

norma ISO Guide 73 (de análise de risco) para apoiar o desenvolvimento e estruturação do processo. Estes padrões garantem a adequação do ambiente de TI às regulamentações apoiadas por leis como BASILEIA e Sarbanes Oxley. O ambiente de TA esta sendo diretamente impactado pelos mesmos fatores externos, sendo impulsionado pela crescente utilização das tecnologias de TI para a gestão do processo de Automação. Desta forma, a criação de normas específicas pelos comitês da ISA, através da S99 e da S100 (Wireless Network), assim como a criação de padrões pelo departamento de Homeland Security dos EUA através do Process Control System Forum, entre outras iniciativas, demonstram a preocupação dos gestores e técnicos na padronização.

A utilização das normas da ISA e do PCS Forum, em conjunto com os frameworks adaptados de TI supracitados, garante uma boa receita na implementação do processo de gestão dos ativos de TI no ambiente de automação.

A ISA está elaborando a SP99 (draft), uma série de quatro normas, cada uma abordando determinado aspecto da segurança da informação em sistemas de controle e de gestão de manufatura. Segundo ISA-SP99,[2] sistemas de controle e de gestão de manufatura incluem todos aqueles sistemas que podem afetar ou influenciar a operação segura e confiável de um processo industrial. Eles incluem sistemas de controle distribuído, PLC's, SCADA, dentre outros. As quatro normas em elaboração são:

- ISA 99.00.01: define escopo, conceitos, modelos e terminologia;
- ISA 99.00.02: define um guia para se estabelecer um programa de segurança para sistemas de manufatura e controle;
- ISA 99.00.03: define como o programa de segurança deve ser executado, após definido e implementado;
- ISA 99.00.04: define os requisitos de segurança para sistemas de manufatura e controle, enfatizando características que diferenciam estes sistemas dos sistemas tradicionais de TI.

Além das normas, o comitê desenvolveu e lançou dois relatórios técnicos:

- TR 99.00.01: contém o estado atual da segurança em sistemas de manufatura e controle, e tecnologias para protegê-los;
- TR 99.00.02: define escopo e fundamentos do que virá a ser a parte dois da norma ISA 99.

A NIST (National Institute of Standards and Technology) vem elaborando a norma SP800-82. Segundo NIST,[3] esta norma é um guia para o estabelecimento de sistemas de controle industrial seguros, incluindo sistemas SCADA, sistemas de controle distribuído, e configuração de outros sistemas de apoio. São identificadas ameaças e vulnerabilidades típicas a estes sistemas, e são recomendadas medidas para mitigar os riscos associados.

Projeto de Separação das Redes de TI e TA

Atualmente, grande parte dos equipamentos de automação que comunicam dados em rede está conectada na rede de dados corporativa. A disponibilidade, desempenho e segurança destes equipamentos, e, portanto dos processos industriais suportados estão vinculadas à infra-estrutura da rede corporativa.

Com a finalidade de fazer o levantamento da situação atual e determinação de metodologia e recursos necessários à implementação da rede de automação da V&M do Brasil, uma consultoria especializada foi contratada. Ela deveria fornecer

documentação com soluções que permitissem a programação posterior da segregação das redes TI/TA.

O trabalho iniciado em 2004 realizou o levantamento da estrutura da rede física e lógica, inventário de hardware e software de cada micro da automação, nível de tráfego entre o ambiente de automação e entre este com o nível corporativo (MES, etc.), políticas de segurança da V&M e necessidades em geral, tais como servidor de arquivos, acesso remoto, segurança, etc.

Realizaram-se ainda as análises da compatibilidade hardware e software dos micros de automação com o Windows 2003 e/ou Windows XP, análise da compatibilidade dos micros de automação e impactos de uma possível mudança de VLAN e, conseqüentemente, no endereçamento de rede.

Com base nos levantamentos executados definiu-se a infra-estrutura física necessária para a implantação da rede de automação separada da corporativa, a solução de firewall para o controle de acesso entre as duas redes, a estrutura de VLANs para a automação de forma a causar o mínimo impacto possível, a especificação dos servidores de domínio da automação e a estratégia de migração para a nova rede.

Como resultado da consultoria também houve a proposição de um WBS – Work Breakdown Structure contendo uma série de atividades mínimas necessárias para a implementação da arquitetura proposta e uma estimativa inicial de prazo para sua execução. Tais informações foram utilizadas para a composição de um cronograma envolvendo desde a aquisição dos ativos e contratação dos responsáveis até a implementação propriamente dita.

A gerência do projeto ficou a cargo da Engenharia de Automação, com a participação efetiva dos membros do COMAUT.

Tecnologias Empregadas

Para tornar viável a migração dos equipamentos localizados na infra-estrutura de rede física da TI para a TA é necessária à criação de arquitetura tão ou mais confiável em termos de disponibilidade, em relação à situação anterior. Assim, para a composição desta infra-estrutura de rede foi utilizado o modelo hierárquico de três camadas proposto pela Cisco. Também conhecido como ECNM – *Enterprise Composite Network Model*,[4] este modelo sugere a divisão da rede em três níveis: *Core* (núcleo), que compõe o backbone da rede e provê comunicação entre sites, *Distribution* (distribuição), que provê a comunicação entre o nível Core e a camada inferior, suportando políticas de acesso mais restritivas, e a camada *Access* (acesso), que garante acesso aos usuários e grupos de trabalho.

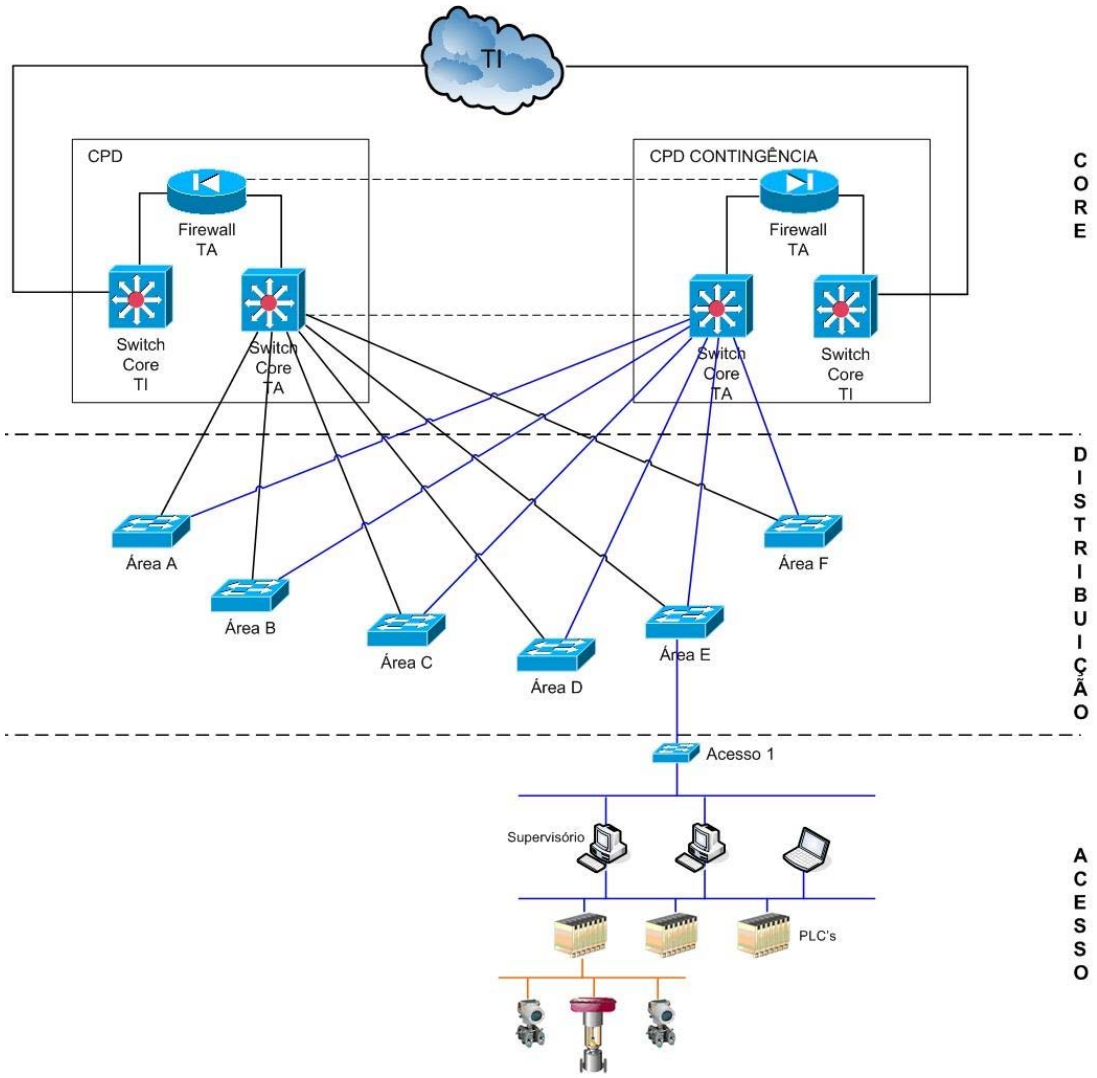

Figura 2 - Modelo Hierárquico de Rede da TA da V&M

A Figura 2 apresenta a topologia de rede composta de acordo com o modelo hierárquico na rede TA da V&M do Brasil. Toda comunicação com o mundo corporativo é realizada através de firewalls, que, efetivamente, realizam a filtragem de todo o tráfego de entrada ou saída, além do tráfego entre as áreas de automação. Desta forma é possível criar regras específicas para a TA sem a necessidade de intervenção em equipamentos de rede da TI e sem que a equipe de suporte corporativo seja envolvida, garantindo autonomia no controle de segurança para quem, de fato, é responsável e tem conhecimento para determinar quais tipos de dados correspondem à automação e, portanto, devem ser permitidos ou não.

Juntamente com switches *Multilayer*, ou multicamadas, os firewalls compõem o *Core* da rede, que, como garantia de alta disponibilidade (*HA – High Avaliability)*, é física e logicamente dividido em dois sites redundantes: CPD e CPD de contingência. Esta arquitetura acompanha o esquema de redundância (*Spare)* disponível no *Core* TI, o que significa que, em uma eventual necessidade de uso dos recursos do site de contingência, também todos os recursos corporativos serão contingenciados. Através do recurso de *failover* (tolerância a falhas) disponível nos firewalls, em caso de falha, não há necessidade de reconexões na camada de aplicação, tornando todo o "chaveamento" transparente para os softwares em uso na automação.

Na camada de distribuição, seis switches dão suporte à conectividade para seis áreas de produção, sendo cada um destes conectado simultaneamente ao core através de links de fibra ópticas redundantes e fisicamente independentes.

Na camada de acesso estão os switches das áreas, servindo como pontos de conexão para equipamentos de nível 2 como, por exemplo, estações de supervisão, estações de manutenção e servidores de comunicação do PIMS. Todo o tráfego é segmentado logicamente através de VLANs de nível 2 e nível 3 (em relação ao modelo OSI), o que impede que domínios de broadcast de outras áreas causem processamento desnecessário (*overhead*) nos equipamentos de automação.

A parte de controle de acesso lógico foi implementada através do serviço de diretórios da Microsoft Active Directory ®. Para assegurar a autonomia das áreas de automação, a infra-estrutura de domínios foi projetada com seis domínios independentes. Cada uma das áreas, desta forma, torna-se responsável pela "liberação do acesso" para usuários ou equipamentos de outras áreas onde esta comunicação inter-áreas eventualmente se faça necessária, o que é feito através do estabelecimento de relações de confiança externas.

Além da segmentação de rede e da implementação de controle de acesso lógico, foram instalados outros controles de segurança no ambiente de automação da V&M durante a execução do projeto. A Tabela 1 apresenta um resumo dos principais controles implementados e a sua relação com as normas disponíveis para a segurança na automação:

Tabela 1 - Principais Controles de Segurança Aplicados Durante o Projeto de Separação das Redes

Controle	Norma Relacionada	Descrição
Procedimentos de controle de acesso: Autenticação através de Senha	Recomendado para sistemas de manufatura e controle de acordo com Relatório ANSI/ISA-TR 99.00.01-2004 e dISA-99.00.02 (Draft)	Serviço de autenticação e autorização implementado através do Microsoft Active Directory
Procedimentos de controle de acesso: Autorização	Prática recomendada pelo dISA-99.00.02	Implementação de políticas de segurança através do Microsoft Active Directory
Segmentação da Rede	Prática recomendada pelo dISA-99.00.02	Segmentação de acordo com o modelo hierárquico de 3 níveis
Firewall Dedicado	Relatório ANSI/ISA-TR 99.00.01-2004	Firewall dedicado à automação implementado com recursos de alta disponibilidade
Virtual Local Área Networks (VLAN´s)	Relatório ANSI/ISA-TR 99.00.01-2004	Segmentação dos domínios de broadcast da automação através de VLAN´s
Detecção de Código Malicioso	Relatório ANSI/ISA-TR 99.00.01-2004	Implantação de software antivírus nas máquinas de automação e servidores de atualização de vacinas nas áreas
Gerenciador de Atualizações	Prática recomendada pelo dISA-99.00.02 no capítulo de ferramentas de segurança (*Security Tools*)	Implantação de software gerenciador de atualizações através do WSUS (*Windows Server Update Services*)
Restrições de acesso a recursos corporativos	Atividade considerada de baixo custo e alto valor, de acordo com dISA-99.00.02	Bloqueio do acesso a Internet e E-mail a partir de estações de automação

METODOLOGIA

O projeto foi dividido em três etapas: Infra-estrutura física, aquisição de ativos de rede e implementação da rede lógica, sendo cada etapa realizada por uma empresa diferente:

- Infra-estrutura física: esta etapa destinada à criação de uma infra-estrutura física de cabeamento lógico segregado para a rede de TA, com execução na usina Barreiro de serviços de lançamento de aproximadamente 20 km de cabos ópticos. Os serviços compreenderam o fornecimento de racks com distribuidores ópticos (DIOs) e acessórios (patch panel, organizadores de cabos, bandejas, régua de tomadas, placas cegas, etc.) assim como infra-estrutura de eletrodutos e/ou canaletas, instalados de acordo com os melhores padrões relacionados. Toda a estrutura de cabeamento resultante passou por testes para certificação de conformidade com normas como TIA/EIA 568-A e ISO 11801;
- Aquisição de ativos de rede: etapa destinada à aquisição dos equipamentos de rede (Firewalls, Switches, etc.), servidores e estações de trabalho;
- Implementação da rede lógica: etapa destinada à implementação propriamente dita do conteúdo especificado. A implementação foi dividida nas seguintes atividades macro:
    - Instalação dos equipamentos de rede e configuração da topologia, aplicando-se controles de segurança de rede indicados com ênfase nos aspectos de disponibilidade;
    - Revisão e execução do plano de migração de IP´s, adequando as áreas a um padrão de endereçamento escalável e adequado às necessidades da automação;
    - Implementação da infra-estrutura de domínio Microsoft de acordo com as características de segurança necessárias para o ambiente de automação;
    - Definição do framework de segurança e execução de auditoria para verificação de aderência do ambiente implementado às melhores práticas de segurança da informação através de utilização de um software especializado de análise e gestão de riscos.

Nas etapas de implementação do Projeto de Separação de Redes, em razão da já mencionada necessidade de tratamento diferenciado para mudanças em ambientes de automação, uma série de cuidados adicionais foram adotados para minimizar a interferência dos trabalhos nos processos produtivos:

- Respeito ao calendário de paradas: todas as intervenções cujas alterações resultassem em necessidade de parada dos equipamentos críticos foram planejadas para execução em datas nas quais tais ambientes já estivessem inoperantes;
- Instalação gradativa da topologia de rede: a topologia de três níveis da TA foi implantada em etapas. Em um primeiro momento o novo Core TA foi implantado “em paralelo” com a estrutura antiga, sem impacto para os equipamentos nela conectados. Com esta estrutura disponível foi possível executar as migrações área por área para a instalação dos switches de distribuição (cuja instalação também foi feita “em paralelo” com a estrutura original) e switches de acesso;
- Testes de laboratório: todos os equipamentos novos utilizados passaram por testes de laboratório. O mesmo ocorreu com os mecanismos de failover, para equipamentos cujos impactos eram desconhecidos para a instalação de

antivírus e atualizações do sistema operacional e para as configurações de domínio e diretivas de grupo (*Policies*);

- Planejamento e documentação: todas as atividades de migração foram precedidas por dias de planejamento com ativa participação dos responsáveis técnicos das áreas. Antes de cada intervenção, documentos contendo a descrição exata das atividades em cada um dos locais eram validados pela equipe do projeto e da área;
- Implementação estratégica das regras de acesso do firewall: para a execução desta etapa crítica do projeto, uma vez que o bloqueio do firewall pode causar interrupção direta de processos de comunicação eventualmente não levantados nas etapas de mapeamento, foi utilizada uma estratégia de implantação de regras de reduzido risco de parada. Inicialmente os firewalls foram instalados com regras de permissionamento completo de tráfego, ou seja, sem bloqueios. Paralelamente, servidores de log (*Syslog Servers*) foram configurados para auditar todo o tráfego de entrada e saída de todas as áreas, o que foi realizado durante um percentual significativo do tempo total do projeto. Decorrido o tempo suficiente para uma medida confiável, foram gerados relatórios sumarizando as conversações de maior freqüência (IP origem, IP destino, protocolo e portas). Sobre estas informações, em conjunto com o mapeamento já realizado sobre as formas de acesso de/para as áreas, foram elaboradas as regras de acesso para a validação pelos responsáveis por tais equipamentos. Ao final, dentre as últimas atividades do projeto, foi realizada a implantação das regras de acesso de forma gradativa e por área;
- Forte uso de gerência de projetos: a criticidade do projeto em relação às variações de, sobretudo prazo, em razão das peculiaridades pertinentes às mudanças para conformidade com o calendário de paradas, exigiram o forte uso de técnicas de gerência de projetos com ênfase na gerência do atraso e custo.

RESULTADOS

Com a evolução do projeto até o presente momento, foi possível verificar que a V&M do Brasil alcançou os seguintes objetivos:

- Envolvimento dos interessados no projeto garantindo o suporte necessário para finalização;
- Adequação da estrutura de rede da TA de acordo com a proposta estabelecida pelo Comitê de Automação;
- Planejamento e implementação do novo modelo de endereçamento IP e domínios;
- Documentação de toda a rede existente, através da realização de inventario de ativos, desenhos, descrições, etc;
- Migração de sistemas legados que estavam sendo executados em sistemas operacionais Windows NT e 98;
- Composição de um modelo de rede com alta disponibilidade, desempenho, entre outros;
- Definição e implementação do padrão de configuração de segurança dos ativos conforme melhores práticas de segurança;
- Adequação do hardware e software especificado para a implementação.

A integração das áreas da V&M pela amplitude do projeto permitiu a discussão de outros projetos de padronização que poderão contribuir ainda mais com os processos da empresa.

CONCLUSÃO

Embora a V&M não tenha nenhuma lei ou regulamentação externa que obrigue a conformidade da área de Automação com os frameworks ou normas citadas, com este projeto, a V&M estabelece um novo padrão para a sua infra-estrutura de automação.

As grandes dificuldades encontradas e lições apreendidas deste projeto foram:

- Obsolescência de parte da especificação: devido a uma alteração estratégica das prioridades da empresa, houve um atraso de quase dois anos entre o planejamento realizado pela consultoria e a sua execução propriamente dita. Como conseqüência, parte da especificação envolvendo levantamentos de infra-estrutura, hardware e software tornou-se obsoleta, causando retrabalho;
- Instabilidade do cronograma de paradas: o calendário de paradas das áreas de automação é vinculado às necessidades específicas de cada área, podendo variar de acordo com a demanda. Tais mudanças nas datas acarretaram impactos no planejamento da execução e no próprio cronograma do projeto, que sofreu diversas alterações para se adequar à situação;
- Oscilações do escopo do projeto em razão de procedimentos operacionais: dentre as atividades levantadas no escopo original surgiram atividades,como reuniões para aprovações de mudanças, não previstos com significativos pacotes de trabalho na divisão do WBS. Como solução, o cronograma foi modificado para se adequar a estas necessidades.

  Ao termino do projeto, a V&M do Brasil espera encontrar o seguinte cenário:
  - As redes de TI e TA separadas lógica e fisicamente;
  - As redes nível 1 e 2 da automação separadas;
  - Um processo de gestão de segurança e de TI separado por unidade de negócio;
  - Todo o projeto de redes documentado.

Conclui-se, também, com este projeto:

- Planejamento: O planejamento de projetos de TI em ambientes de TA deve levar em consideração as necessidades específicas da automação, com processos de mudança gradativos e bem planejados, considerando sempre o calendário de produção e com análises de risco da mudança para o processo produtivo;
- Controles de segurança para a TA: ao definir a estratégia de segurança para o ambiente de TA é essencial levar em conta as diferenças entre o que é aplicável para TI e TA, definindo-se quais os aspectos de segurança devem ser priorizados e quais são realmente possíveis na automação e utilizando, sempre que possível, testes que validem a aplicabilidade do controle sem interferências;
- Preparação adequada para as etapas de migração: como as janelas de parada dos processos produtivos para intervenções são, normalmente, estreitas, um bom planejamento das etapas de migração deve ser realizado para que o uso deste tempo seja otimizado e problemas potenciais possam ser previstos;

- Clareza em relação às atividades executadas: o uso de forte interação com os responsáveis técnicos pelas áreas de automação, aliado à clareza e transparência nas atividades e seus objetivos facilita a atenuação do receio e aversão à mudança que naturalmente existe dentre os profissionais de TA, facilitando a execução dos trabalhos na medida em que ocorre uma maior compreensão dos benefícios esperados;
- Adequação às normas: há atividades necessárias para adequação a algumas normas como a ISO 27000 que são de baixo custo e esforço para implementação. Atividades como a realização de inventário pode ser realizada em projetos deste porte sem muita interferência nas tarefas já planejadas.

Trabalhos Futuros

A V&M entende que ao término do projeto deverá ser elaborado um processo de gestão, da nova arquitetura criada, envolvendo a gestão de segurança da informação . Estas atividades deverão ser planejadas nos últimos meses do projeto, de forma a permitir a correta adequação das áreas.

A V&M também deverá planejar a implementação de outros controles de segurança não planejados no projeto, assim como estabelecer um processo de gestão de risco.

No intuito de se adequar a possíveis regulamentações a V&M poderá utilizar o COBIT ou a ISO/IEC27000: 2005 [5] para estabelecer os controles de governança de TI e segurança do processo de gestão.

REFERÊNCIAS

1 NOGUEIRA JUNIOR, K. A, ALMEIDA, E. M. A Estrutura Organizacional da Automação na V&M do Brasil, X Seminário de Automação de Processos – ABM. Outubro de 2006 – Belo Horizonte/MG.

2 ISA, ISA-SP99, Manufacturing and Control Systems Security, disponível em <http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821>, acessado em 27/06/2007.

3 NIST, Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security, disponível em <http://csrc.nist.gov/publications/drafts/800-82/Draft-SP800-82.pdf> acessado em 27/06/2007.

4 CISCO, Building Cisco Multilayer Switched Networks (BCMSN) V. 3.0 2006 – Student Guide, pag. 1-18

5 ISO, ISO/IEC 27000:2005.

BIBLIOGRAFIA

1 V&M DO BRASIL S.A.; Plano Diretor de Automação e Informação. Outubro de 2004.