TECNOLOGIAS DE SEGURANÇA E DETECÇÃO DE VULNERABILIDADES EM SISTEMAS DE AUTOMAÇÃO METROVIÁRIA

Gilmario Ribeiro

Bruno Leça Ribeiro

20ª SEMANA DE TECNOLOGIA METROFERROVIÁRIA

PRÊMIO TECNOLOGIA E DESENVOLVIMENTO METROFERROVIÁRIOS

CATEGORIA 3

“ Tecnologias de Segurança e Detecção de Vulnerabilidades em Sistemas de Automação Metroviária ”

INTRODUÇÃO

O setor de transportes é considerado pelo Governo Federal como sendo uma infraestrutura crítica, cuja definição dada na portaria nº 25, de 27 de abril de 2010 e emitida pelo Gabinete de Segurança Institucional, indica que se tratam das instalações, serviços, bens e sistemas cuja interrupção ou destruição, total ou parcial, provocará sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade.

Dadas as proporções do serviço que um Metrô presta e sua área de abrangência na Região Metropolitana, pode-se considerar o seu parque de ativos , como parte da infraestrutura crítica desta área de abrangência e da mesma forma, seus sistemas, como algo essencial para o funcionamento da cidade.

Justifica-se então o emprego de métodos adicionais de segurança aos sistemas que possuem interconexões de comunicação, uma vez que somente ações comuns não garantem um monitoramento permanente dos riscos e das vulnerabilidades embutidas nas tecnologias.

Atualmente devido a tendência de conectividades múltiplas, existem várias formas de ataque às redes e sistemas, bem como, no contra ataque, bons sistemas de detecção e prevenção a estes eventos. Porém, de nada adiantaria disponibilizar sistemas de segurança, se não houver sua monitoração e seu gerenciamento permanente.

Nos desafios à segurança da informação há a disputa pelo poder entre equipes com responsabilidades distintas sobre a rede e a segurança, principalmente quando há ambientes de TI (Tecnologia da Informação) e de TA (Tecnologia de Automação) envolvidos nesta missão, e sendo de grande importância a criação de um CSIRT (Comissão de Segurança para Tratamento e Respostas a Incidentes), envolvendo integrantes de áreas distintas, nos moldes de uma equipe multidisciplinar composta por técnicos, analistas, engenheiros ou especialistas e consultores com conhecimentos em:

- Telecomunicações: redes SDH, Ethernet e wireless, comunicação, protocolos de roteamento, Arquiteturas Modelo OSI; endereçamento IP, VLANS, acesso remoto;

- Sinalização, Controle: características de equipamentos, interação entre sub-sistemas;

- Trens: redes industriais, Ethernet e wireless, comunicação de dados, protocolos de roteamento, automação, CPLs;

- Sistemas operacionais: Windows Server, Linux, Unix etc;

- Segurança da informação: métodos utilizados em invasões, análise de riscos e vulnerabilidades, auditoria, técnicas e tecnologias de prevenção e identificação de ataques, execução e administração de backups, técnicas de autenticação. IDS, IPS, Site Survey etc;

- Gestão de redes e Segurança dos serviços: ITIL, COBIT, ISO 27000, ISA-99.

Os novos sistemas metroviários englobando equipamentos fixos e material rodante, já utilizam plena comunicação por meio de Redes de Computadores, contendo as diferentes tecnologias de transmissão de dados, sejam elas cabeadas, ópticas e inclusive as sem fio.

Esta condição traz à tona uma forte preocupação com a disponibilidade e integridade das informações, pois se não forem aplicadas as mais recentes técnicas de segurança nas redes e nos sistemas, podemos ter surpresas englobando questões sérias , por possíveis vulnerabilidades desconhecidas ou ainda não mapeadas, tipo dos exemplos abaixo:

1 http://info.abril.com.br/noticias/seguranca/trojan-contribuiu-com-queda-de-aviao-espanho-20082010-34.shl

2 http://www.sicherheitstacho.eu/?lang=en

3 http://www.tecmundo.com.br/selecao/38267-os-5-maiores-desastres-militares-envolvendo-computadores.htm

4 http://www.tecmundo.com.br/tecnologia-militar/37801-exercito-deve-receber-r-400-milhoes-para-prevencao-de-guerra-cibernetica-.htm

5 http://www.istoedinheiro.com.br/noticias/economia/20140710/hackers-chineses-atacam-base-dados-governo-americano/170417.shtml

6 http://www.tecmundo.com.br/seguranca/46926-estacao-espacial-internacional-e-infectada-com-o-virus-stuxnet.htm

7 http://www.digitalattackmap.com/#anim=1&color=0&country=ALL&time=16235&view=map

Esta abordagem é uma pequena amostra de tais preocupações e necessidades, bem como uma síntese de discussões envolvendo Tecnologia em Segurança de Redes e Sistemas Computacionais de natureza operacional (ambiente de automação).

Considera-se para esta denominação, o acervo 'não administrativo' de Computadores, Notebooks, Tablets, TPDs, Ativos de Redes (switch, hubs, roteadores, access-points, conversores etc), Armários, Racks, Servidores, Antenas, PLCs, Dispositivos de leitura e armazenamento de dados, Softwares, Periféricos, Nobreaks, Monitores, circuitos eletrônicos utilizados em ações diretas em equipamentos embarcados nos trens, armários de

transmissão e telecomunicações, instrumentos e dispositivos elétricos em estações, de sinalização, tração, energia, entre outros.

Todos esses dispositivos fazem parte de um acervo computacional, hoje utilizados em rotinas e processos de Operação e Manutenção, aplicados ao sistema metroviário, não controlados pela área de TI, mas que entretanto devem ser também objeto das políticas corporativas, aplicáveis aos equipamentos de uso administrativo, obedecendo as rotinas de segurança para prevenir possíveis vulnerabilidades existentes ou desconhecidas.

Contém softwares dedicados de automação, sinalização ou aplicativos de natureza específica metroferroviária, que gradativamente com o tempo evoluíram de sinais ANALÓGICOS e ISOLADOS, para sistemas DIGITAIS e INTEGRADOS que usam inclusive, comunicações sem fio via rádio frequência (WiFi) de diversos padrões, inclusive os de mercado.

Antenas wireless do novo sistema de sinalização dos trens do Metrô

No entanto, para a implementação de novas tecnologias no cenário metroferroviário, visando a realização direta ou indiretamente de um transporte de passageiros com maior eficiência, estão sendo inseridos diversos equipamentos que dependem da tecnologia de redes de comunicação e transmissão de dados, sejam em padrões proprietários ou públicos.

Abordamos preocupantes reflexões envolvendo as vulnerabilidades da Tecnologia da Informação (inerentes do mundo de TI), hoje bastante presente nos ambientes de Automação, onde este (TA) encontra-se ainda pouco preparado para lidar com eficientes contramedidas (hardwares, softwares e redes), através de um gerenciamento seguro, ativo e contínuo deste acervo computacional, aplicado em missões críticas.

Vulnerabilidades em Sistemas de Automação

As abordagens abaixo refletem informações e orientações importantes e necessárias:

- falta de monitoramento em tempo real = análise logs;

- segmentação do desenvolvimento da rede operacional com a corporativa = Vlans;

- controle de portas USBs nos ativos de rede;

- controle de mídias removíveis junto aos usuários;

- controle de uso de computadores externos, rede para visitantes etc = NAT;

- central de avaliação de logs, de forma coordenada e não isoladamente;

- controle das redes WiFi e sem haver conexão destas, com os ativos de automação;

- verificação da abrangência de sinal de forma a ser tecnicamente controlado;

- controle de acessos e verificação de requisitos de segurança para redes sem fio, equivalentes aos de uma rede cabeada e com a implantação de certificados digitais;

- estabelecimento de check lists norteados na base de conhecimento para analise em planilha pontuada, permitindo avaliações de segurança (RIPT);

- utilização de manual para desenvolvimento seguro na implantação de aplicativos;

- nas necessárias interconexões de redes de TI com TA, o ideal segundo as normas é que hajam 2 Firewalls de fabricantes diferentes, com um conjunto de regras bem configuradas e, protegendo uma DMZ, onde existam servidores para acesso comum de uma rede e de outra, via firewalls respectivos com o principio do menor privilegio, ou seja, negar tudo, exceto aquilo que for permitido em instruções administradas por cada dono do negocio (regras da área de TI para o firewall de TI e regras da área de TA para o firewall de TA);

- a ligação de equipamentos operacionais na rede administrativa é de fato, algo perigoso para ambos os ambientes, mas principalmente para o de TA, exigindo quando isso ocorra, uma permanente monitoração;

- sabotagem em uma tecnologia de rede sem fio de qualquer padrão é algo muito fácil, simples e inevitável e, para um bloqueador de sinais não há solução técnica (Jammers);

- máquinas zumbis (BOTs) executam tarefas obscuras de ataques e anonimamente para seus 'mestres' (crackers), sendo algo valorado e negociado no ambiente da 'deepweb' (internet sem regras e criptografada através da rede chamada Tor);

- a engenhariasSocial e o Dumpster-diving são práticas de coletar informações analisando pessoas e o lixo, onde isso não é considerado como crime;

- discos não mais utilizados devem ser destruídos ou fisicamente apagados através de ferramentas tipo Shredders que fazem isso, gravando 0,1 em todas suas trilhas;

- informações críticas devem ser descartadas quando nas substituições das máquinas do acervo computacional administrativo ou de automação, e criptografadas quando usado dados em mídias removíveis (discos externos, bem como pendrives, CDs etc);

- solução do tipo Checkpoint-go permite acesso remoto mais seguro, via conexões VPN por máquina virtual usando pendrive, através de aplicações homologadas com dupla forma de autenticação, uma via Rede e outra via Token;

- contabilidade em segurança é ums boa maneira de checar os controles e prevenir as falhas através da analise periódica dos logs e, a ausência desta politica resulta em inconsistências na gerência dos ativos e na administração dos controles;

- as politicas de senhas muito exigentes, possuem um custo significativo no ambiente de automação, diferente de TI (custos de gestão, suporte, segurança);

- um processo de Defesa em Profundidade consiste em diagramas de zonas e conduítes, onde entre uma zona e outra, há sempre um dispositivo de segurança parametrizado em 3 níveis, amenizando problemas em tais perímetros:

SLT = security lever (Objetivo dos níveis: 0, 1, 2);

SLA = security lever (nível Atingido: 0, 1, 2);

SLC = security lever (Capacidade de níveis: 0, 1, 2);

- novos conceitos de segurança por projeto vêm sendo desenvolvidos e, nas integrações de infraestrutura, uma central de gerencia interna de segurança, deve ser montada em uma região neutra (desmilitarizada), entre as interconexões das plataformas de TA e de TI;

- um eficiente monitoramento contínuo dos sistemas críticos deve ser feito por diversos motivos, mas principalmente para bem manter, controlar e restabelecer rapidamente os processos vitais, garantindo disponibilidade dos serviços. E tal agente de monitoramento deve propiciar prevenção e antecipação de falhas de hardware, software e infraestrutura.

Algumas medidas rígidas de segurança devem ser utilizadas, tais como uma solução DMZ:

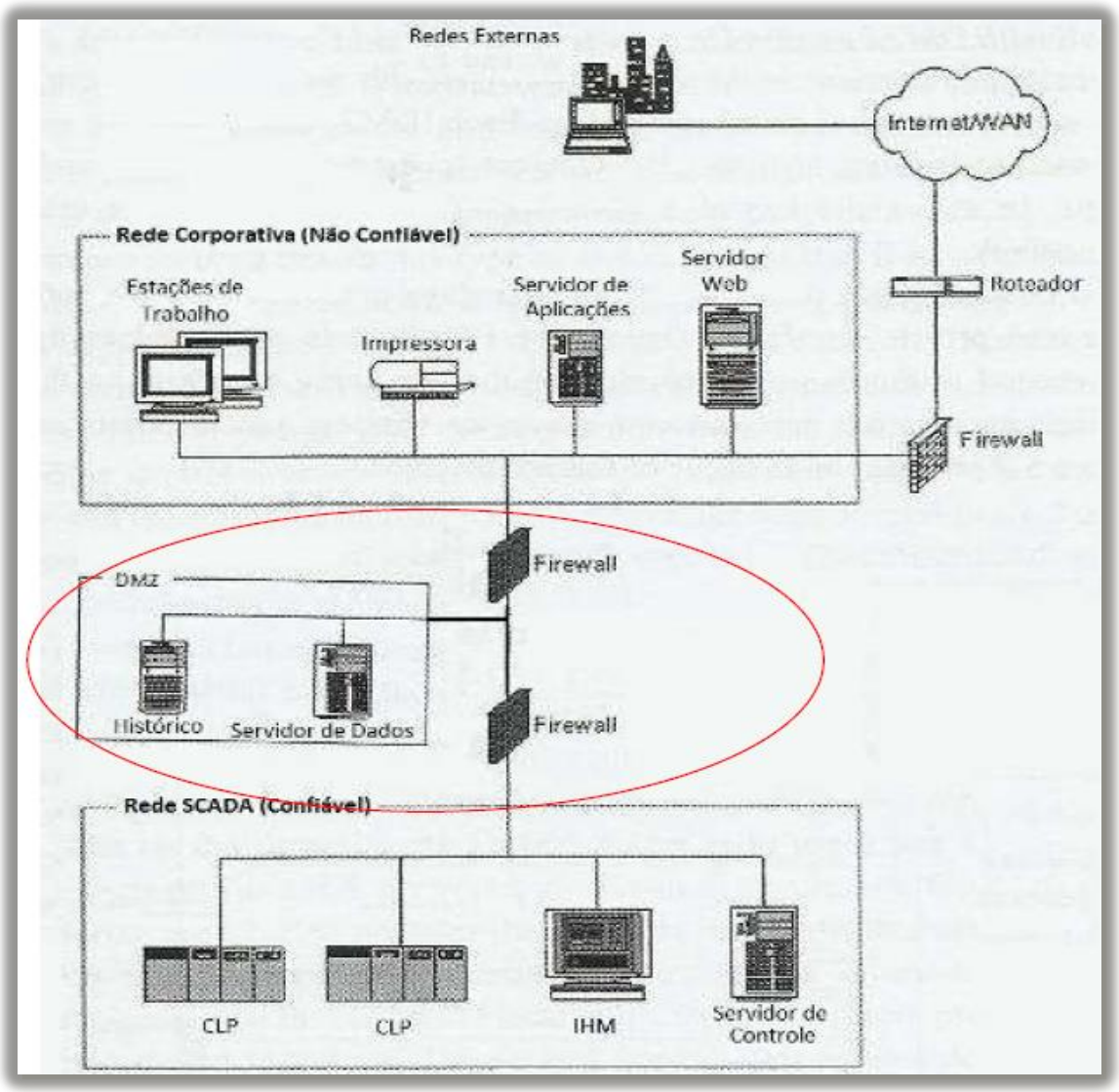
- o uso de 2 Firewalls para a criação da DMZ (Zona Desmilitarizada) permite que cada negócio, controle a segurança de sua infraestrutura de rede e seus sistemas;

- permite uma melhor configuração para conciliar necessidades específicas de TI e TA;

- cada gestor de rede cria e administra suas próprias regras, de acordo com seu negócio.

- adotando Firewalls de diferentes fabricantes, aumenta-se mais ainda a segurança;

- topologia atende diversas necessidades, sendo o padrão suportado pela ANSI/ISA-99.



DIAGNÓSTICO

Capacitação constante é uma importante ação, devido essa disciplina não ser matéria absorvida e dominada pelos colaboradores que atuam diretamente nas atividades de manter disponível, os equipamentos de rede e os sistemas no ambiente técnico operacional.

Importante priorizar a implantação de politicas envolvendo melhoria de processos em controle, gerenciamento e técnicas de segurança, nas rotinas de operação e manutenção dos recursos computacionais (equipamentos, sistemas e redes), instalados no campo.

Nesta análise, tais ações podem ser viabilizadas através da implementação de um Centro de Operações de Rede, baseado em modelos de NOC-Network Operation Center e SOC-Security Operation Center, permitindo gerenciamento da saúde dos ativos e, rapidez no diagnóstico e atuação das áreas de Manutenção Preventiva ou Corretiva, junto à infraestrutura e acervo de hardware e software já instalados ou em futura implantação.

Também necessário um plano geral para disseminação das importantes boas práticas de Segurança no ambiente Metroferroviário, monitorando e administrando cenários remotos do acervo computacional , evitando problemas de Security e impedindo que evoluam ou tornem-se 'efeito dominó ', gerando em cascata, um inesperado problema de Safety.

Recentes informações obtidas em congressos e seminários de segurança da informação, de auditoria, sistemas, governança, bem como de hacking-ativismo em 2013, indicam que:

- 75% das empresas serão infectadas em algum momento de sua existência e 74% das empresas atacadas, reportaram perda de clientes devido a tais fatos;

- 265% foi o aumento de ataques virtuais entre 2011 e 2012, tornando imprescindíveis os investimentos em sistemas automáticos para detecção de vulnerabilidades;

- inevitável a criação de grupo de respostas a incidentes de natureza crítica, pois hoje em dia os crimes são On-Line e as investigações normalmente são Off-Line;

- empresas de governo não devem utilizar serviço de provedores gratuitos tipo Gmail, agenda Google nem hospedar conteúdos em provedor estrangeiro, pois não ter uma estratégia técnica para a segurança, deixou de ser uma opção;

- uma mudança de paradigma é necessária para estabelecer caminhos de controle pois a segurança 100% é algo utópico, onde os técnicos, engenheiros e analistas de segurança das empresas devem ser gestores de risco do negócio da instituição;

- a tarefa de detecção de intrusão não é uma regra estática, pois em épocas de guerra deve-se prever as ações inimigas, onde as plataformas de proteção tornam-se ineficientes sem reais investimentos na cultura e no comportamento dos envolvidos, sejam eles colaboradores internos ou externos;

- de 47 ataques planejados à NASA em 1 ano, 13 foram bem sucedidos com 150 credenciais roubadas, mudando os logs de sistemas internos;

- dos 45 malwares direcionados ao jornal New York Times, somente 1 foi detectado pelo seu anti-virus, vazando matérias de 12 jornalistas antes de sua publicação;

- bancos brasileiros declaram perdas de 1,2 bilhão em fraudes eletrônicas em 2012 e 91% de ataques são direcionados por e-mail, sendo 12% via pdf, 10% doc e 8% jpg;

- 58% das urls no Brasil são vulneráveis e o país responde por 36% dos spams e, segundo a Polícia Federal, crimes digitais já é um negócio maior que o narcotráfico;

- para TA a disponibilidade é o mais relevante no pilar CID da segurança da informação;

- por hora são gerados 8200 novos códigos maliciosos em todo o mundo e, o aumento da atividade criminosa é devido a evolução da infraestrutura digital, 'versus' a estagnação da postura com os assuntos de segurança;

- quanto mais tecnologia se emprega aos processos corporativos, mais necessidade há de investimentos na Segurança desta mesma tecnologia recém adotada.

Afirma-se que com as facilidades do mundo digital, a fim de se manter seguros e protegidos seus dados, a maioria das empresas devem se utilizar de tecnologias avançadas para proteção de seus ativos tangíveis e intangíveis.

Tais soluções devem ir desde um simples anti-virus, até os complexos sistemas de criptografia, aliados a potentes regras de firewall ou implementação de sistema para detecção de intrusos (IDS), ou de proteção (IPS).

Uma falsa sensação de segurança existe permeando os meios corporativos, quando se defende a máxima de que redes isoladas, segregadas ou não conectadas estão protegidas. Essas afirmações são pseudo verdades, uma vez que a maioria das vulnerabilidades são causadas por agentes em ambientes internos da corporação, com acesso e informação privilegiada, conforme pesquisa de 2009 divulgada pela KPMG em figura a seguir.

ANÁLISE

Para se garantir um nível adequado de segurança, gerenciamento dos ativos e gestão dos riscos para estas novas tecnologias, é necessário um reconhecimento efetivo da natureza problemática desta questão, formalizando e designando atribuições de competências específicas, tais como em Políticas e em Técnicas de Segurança Física/ Lógica, objetivando uma regência harmônica e integrada de todos os sistemas e redes operacionais.

Nesta análise, tais ações podem demonstrar a possibilidade em se implementar um Centro de Operações baseado em modelos de NOC-Network Operation Center e SOC-Security Operation Center, permitindo rapidez no diagnóstico e atuação das áreas junto à infraestrutura e ao acervo de hardware, software e redes operacionais.

Discussão de exemplos e casos sobre insegurança e vulnerabilidades em sistemas, ocorridos nos meios aéreo, industrial, governamental, bancário, petrolífero etc, em paralelo com a preocupante realidade tecnológica no segmento de transporte de massa (aéreo, trem, metrô, monotrilho), caracterizando uma necessidade da implantação de tais plataformas e políticas de segurança, englobando todo o ambiente corporativo (administrativo e campo).

A formação em especialidades também deve preparar profissionais para atuar no ramo da Segurança de Redes e Sistemas, principalmente os utilizados na automação da operação comercial, em seu aspecto amplo.

Isto vale desde a especificação e discussão de tecnologias a serem concebidas e aplicadas em diversos contextos de plataformas computacionais, até a análise das situações de risco da segurança e a gestão de processos e pessoas relacionados com a questão de security na utilização dos diversos sistemas críticos do negócio.

Portanto uma capacitação e atualização contínua dos profissionais que atuam em áreas de Projeto, TI, Manutenção e Operação tornam-se fundamentais, em especial junto aqueles que tratam diretamente com os sistemas vitais e críticos, em especial os sistemas de transmissão de dados e os de sinalização com interação entre Trens, Estações e Centro de Controle, bem como os de subestações de energia elétrica.

E apenas o controle e sinalização baseados em redes e equipamentos dedicados e independentes, não exige ou permite um monitoramento de suas funções de gerência.

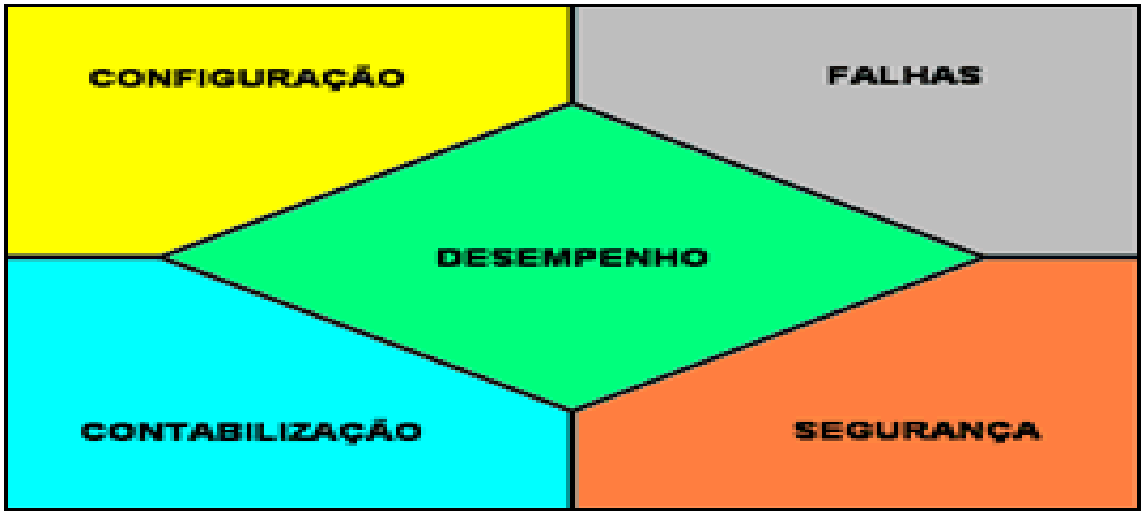
Estas características de segregação eram suficientes para as necessidades operacionais antigas e, devido à forma de atuação das áreas , não se fazia necessário investir na implantação de um sistema de gerenciamento da comunicação entre equipamentos e Centro de Controle, nem da criação de postos dedicados à monitoração e segurança.

Porém atualmente, com o uso de novas tecnologias este cenário já mudou bastante.

http://www.flightradar24.com/

CONCLUSÃO

É de extrema importância o emprego de sistemas IDS e IPS em todos os cenários computacionais, principalmente no operacional e em redes sem fio, por estes oferecerem um grande número de dispositivos capazes de capturar seu sinal, tornando-o disponível no interior dos trens, estações e vias, constituindo-se em uma grande fonte de vulnerabilidade, onde atrasos e interrupções podem comprometer sistemas embarcados de voz e vídeo.



Áreas funcionais do Gerenciamento de Redes

E três campos básicos a serem gerenciados em uma rede são normalmente elencados:

- Falhas: envolve identificar e isolar a falha, faz uso de ferramentas de gerenciamento que possibilitam a automatização dos processos, desde identificação até total correção da falha;

- Desempenho: permite identificar uma má utilização da rede e fornece informações para o planejamento de aumento/capacidade, diminuição de custos e necessidade de melhorias;

- Configuração: gerenciada de forma centralizada, facilita a administração de dados complexos e de diversos equipamentos.

Especialistas afirmam que numa rede composta por equipamentos de modelos e fabricantes diferentes, os custos da equipe serão muito altos, se a operação e manutenção forem de forma descentralizada. E a recomendação M20 do ITU-T aconselha que a manutenção centralizada deva ser considerada, ao especificar novos sistemas de telecomunicações e seus equipamentos, onde enumera diversos benefícios:

- flexibilidade para organizar as operações de manutenção e administração;

- uso mais eficiente de recursos humanos altamente qualificados;

- uso mais eficaz dos dados e das bases de dados;

- o uso de terminais remotos possibilita escolher de forma tranquila, o melhor local para se instalar o Centro de Gerenciamento, para melhor eficácia e menor custo da manutenção;

- aumento da disponibilidade dos sistemas de transmissão e comutação;

- melhoria geral da qualidade dos serviços prestados.

Da mesma forma, atribui-se mais vantagens à manutenção centralizada, uma vez que é possível realizar atividades remotamente, bem como automatizar tarefas, utilizando um Operational Support System (OSS), software para gerenciamento da rede.

Tudo isso vai ao encontro sobre o que define a TELEBRAS, que caracteriza o gerenciamento integrado como a execução organizada das funções de operação, administração, manutenção e provisionamento de todos os elementos da rede, utilizando a gerência concentrada em local estratégico, para garantia da prestação eficiente dos serviços.

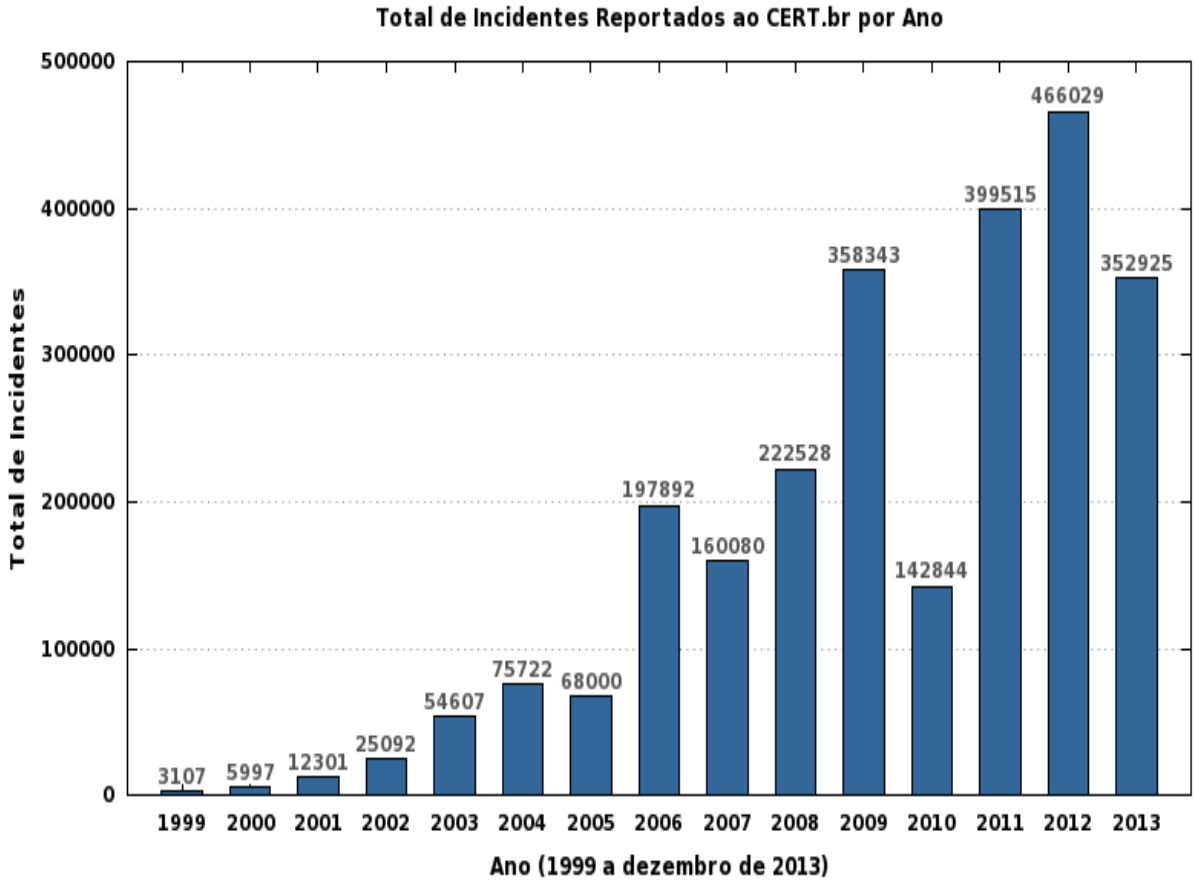
A definição dada pelo CERT.BR (2012) é de que incidentes de segurança são eventos adversos, confirmados ou sob suspeita, relacionados à segurança de sistemas de computação ou de redes de computadores e cita como exemplos, as tentativas de acesso ou uso não autorizado a sistemas ou dados:

- ataques de negação de serviço;

- modificações sem conhecimento/consentimento prévio do dono do sistema;

- desrespeito às políticas de segurança ou de uso aceitável.

O CERT.BR mantém estatísticas de notificações de incidentes de segurança em redes:



Estas notificações de incidentes referem-se às tentativas de fraude, furto de informações e de credenciais, ataques a servidores web, computadores invadidos ou infectados, alteração de arquivos, varredura de portas TCP/UDP, propagação de códigos maliciosos, ataques de negação de serviço e acesso não autorizado à rede.

Devido demandas inevitáveis exigindo a necessidade de integração das redes, torna-se importante considerar que todos os sistemas metroviários que utilizam rede de dados, independente das redes serem ou não isoladas, devem seguir as definições de um padrão, tipo uma Instrução de Projeto para Utilização de Roteamento e Endereçamento IP.

Um Centro de Operações de Rede (NOC), por definição, é um local onde se centraliza a gerência de uma ou mais redes de comunicação, sejam elas públicas ou privadas.

COMMIT–Centro de Operações de Manutenção e Monitoramento de Instalações e Telecomunicações (METRO MADRID/ ESPANHA - 2013)

A partir desse centro e de diversos programas de computador que monitoram a rede, os operadores podem agir numa atuação pontual ou repasse de atuação a outra equipe, em tempo real, gerenciando cada ativo dentro das redes integradas.

Este serviço normalmente é adotado, visto que com o NOC o downtime (tempo de indisponibilidade) é reduzido quase a zero e, com isso as empresas se tornam mais competitivas, passando de uma operação REATIVA, para uma operação PRÓ ATIVA.

Para verificar se o nível de serviço atual corresponde ao desejado, informações são captadas da rede, obtendo a funcionalidade e a performance em tempo real.

As informações são captadas continuamente ou sob demanda, e armazenadas em banco de dados de gerência. Partes destes dados são submetidos à análise e outros utilizados para comparar o status real da rede, com aquele planejado, permitindo verificar as anomalias.

Deve-se preparar uma série de atividades para resolução de problemas, desde uma simples substituição de dispositivo defeituoso, até a execução de ferramentas mais sofisticadas para um diagnóstico mais acurado do problema, além de monitorar a rede de vários tipos, associados a softwares de gerenciamento, atuando na detecção, análise e correção de falhas, de modo a garantir um acordo contratado com os clientes e gerando um book operacional com os serviços executados e ofertados às redes de TI e TA.

E tal aplicação do gerenciamento centralizado, baseada na recomendação M.20 da ITU-T é essencial, principalmente pela dimensão, complexidade e elevada dependência que a operação da empresa tem em relação aos serviços suportados por tais tecnologias de redes.

A seguir, alguns comparativos sobre a evolução do comportamento, dentro da área de TI:

Tabela de Comportamento - Cenário Anterior versus Cenário Atual

Cenário Anterior	**Cenário Atual**
Atendimento do usuário	Atendimento do cliente
Perspectiva interna	Perspectiva externa
Esforço pessoal	Esforço repetitivo e medido
Foco na tecnologia	Foco no processo
Processos ad-hoc	Processos racionalizados
Recursos internos	Recursos internos e externos
Comportamento reativo	Comportamento proativo
Visão fragmentada	Visão integrada
Sistema manual	Sistema automatizado
Gestor de operações	Gestor de serviços

Unificar o monitoramento de equipamentos, serviços e aplicações proporciona maior agilidade, por simplificar os processos de abertura, e gestão das falhas, reduzindo o número de pessoas envolvidas na atuação.

Todas estas atividades podem ser executadas remotamente e de maneira contínua, portanto muito mais eficiente através de um NOC, sendo possível inclusive a resolução de eventuais desvios, sem que haja necessidade do deslocamento de técnicos ao local, permitindo que a equipe de campo possa se dedicar na realização de outras atividades.

Trazendo estes conceitos para a realidade de TA nas áreas do ambiente Metroviário, temos:

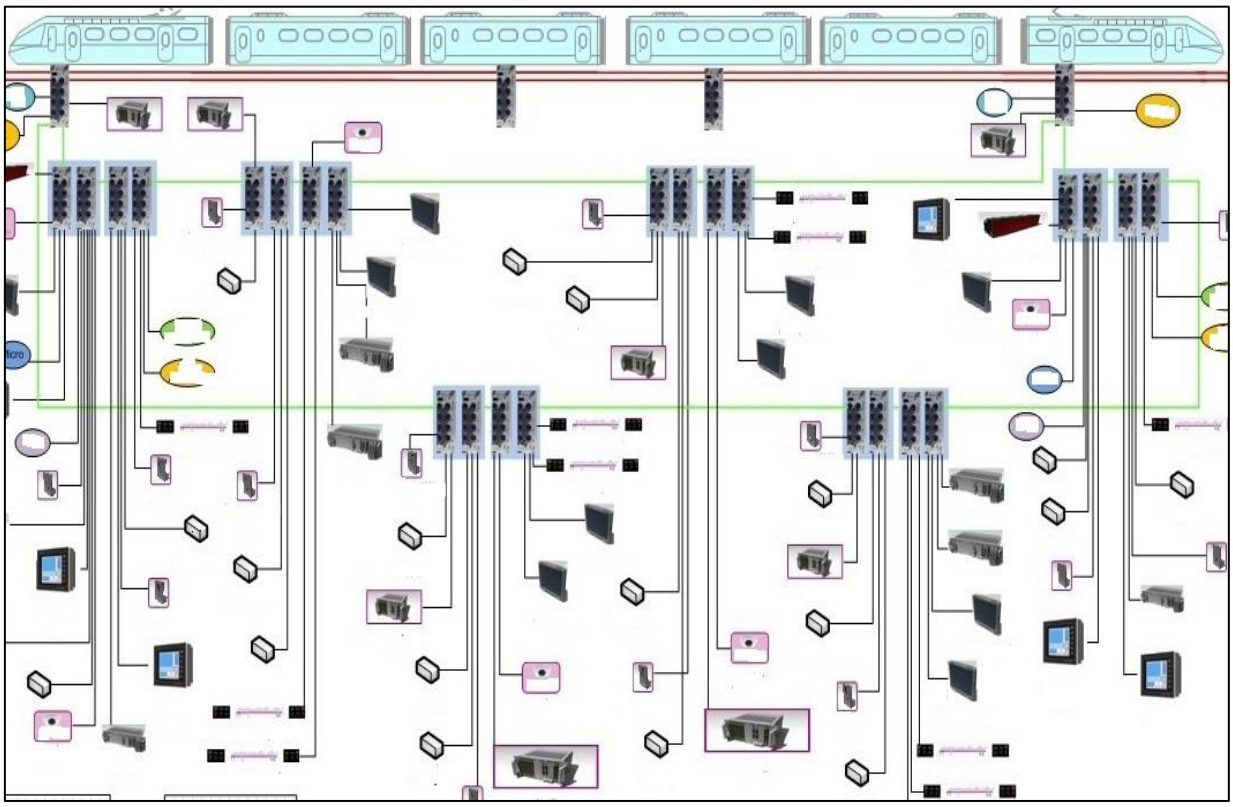
Cenário de Atuações - Atual e Futuro

Cenário Atual	**Cenário Futuro**
Atendimento ao CCO e Estações	Atendimento aos usuários de serviços
Equipamentos da Operação	Equipamentos da Manutenção
Esforço momentâneo	Esforço contínuo
Foco no equipamento	Foco nas redes, sistemas e serviços
Diagnóstico no local da falha	Diagnóstico remoto
Equipamentos dedicados	Equipamentos com múltiplas aplicações
Comportamento reativo	Comportamento proativo
Visão fragmentada	Visão integrada
Instrumentos de medida	Software
Gestão das falhas	Gestão do funcionamento

O fato das aplicações estarem bloqueadas para acesso externo (internet, extranet) pode levar a errônea impressão de que não há muito com que se preocupar.

Porém, estudos revelam que grande parcela do número de fraudadores no Brasil estão dentro da própria empresa. Por isso, devemos nos esforçar para evitar qualquer brecha de segurança, sejam físicas ou lógicas, principalmente nos ambientes internos de automação, que é o cenário dos equipamentos operacionais vitais e de alto impacto nos negócios.

Exemplo de Redes Embarcadas



Reflexões Finais

"...os cyber crimes e as ameaças digitais correm na velocidade da LUZ e as ações envolvendo segurança andam na velocidade da LEI..."

"...quanto mais Tecnologia se implanta, mais necessidade há de investimentos em Segurança, devido as vulnerabilidades decorrentes desta mesma tecnologia..."

"...a pior Segurança é aquela em que se ACHA que JÁ estamos totalmente seguros..."

REFERÊNCIAS

ABNT. ABNT NBR ISSO/IEC 27002 Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação. 2007

ABNT. ABNT NBR ISSO/IEC 27003 Tecnologia da Informação - Técnicas de Segurança - Diretrizes para Implantação de um Sistema de Gestão da Segurança da Informação. RJ, 2011

CERT.BR, Cartilha de Segurança para Internet. Disponível em < http://cartilha. cert.br/ >2006

CERT.BR. Práticas de Segurança para Administradores de Redes Internet. Disponível em < http://www.cert.br/docs/seg-adm-redes/seg-adm-redes.html#subsec4.8 >. 2003.

COMPANHIA DO METROPOLITANO DE SÃO PAULO. NOR-00-204 05 COMISSÃO PERMANENTE DE SEGURANÇA EM SISTEMAS OPERACIONAIS (COPESE) – Intranet Metrô/SP

COMPANHIA DO METROPOLITANO DE SÃO PAULO. Regimento Interno – Intranet Metrô/SP

CSIRT – UNICAMP. CSIRT – Disponível em < http://www.security.unicamp.br/servicos.html >

GABINETE DE SEGURANÇA INSTITUCIONAL. PORTARIA N 25, DE 27 DE ABRIL DE 2010 - Institui o Subgrupo Técnico de Segurança de Infraestruturas Críticas de Transportes Terrestres (SGTSIC-Transportes Terrestres) e dá outras providências. Disponível em < http://www.jusbrasil.com.br/diarios/3661996/dou-secao-1-28-04-2010-pg-162 >

GIAVAROTO, Silvio Cesar Roxo; SANTOS, Gerson Raimundo dos. Backtrack Linux – Auditoria e teste de invasão em redes de computadores. Rio de Janeiro. Editora Ciência Moderna. 2013

TELEBRAS, Prática 501-100-104 Conceitos de Gerência Integrada de Redes e Serviços e Gerência Redes/Telecom http://sistemas.anatel.gov.br/sdt/PraticasTelebras/01438.pdf