*Por Sérgio Sevileanu e Rodrigo Leal**

Capítulo III

Arquitetura da subestação segura

Como implementar os requisitos dos padrões de segurança cibernética em sistemas de automação de energia

Introdução

Os sistemas de automação de energia estão cada vez mais conectados e empregam um número crescente de elementos de hardware e software criados originalmente para uso em ambientes de TI (Tecnologia de Informação), incluindo equipamentos de rede, sistemas operacionais, protocolos de comunicação e até utilitários de software que são incorporados a produtos de automação. Se por um lado, a digitalização e as novas tecnologias abrem caminho para inovação e novas aplicações, elas também aumentam a exposição e a superfície de ataque cibernético destes sistemas, conforme foi dito no primeiro artigo deste fascículo.

Os crimes cibernéticos também têm aumentado em frequência e sofisticação. Atraídos por um mercado aparentemente rentável, organizações criminosas desenvolvem ferramentas para explorar vulnerabilidades em dispositivos e malwares que são introduzidos para efetivar os ataques. O sequestro de dados para cobrança de resgate (ransonware), o roubo de informações e a parada de sistemas (inclusive de automação) estão entre os principais alvos destas organizações.

Um caso recente chamou a atenção da comunidade de segurança devido ao seu amplo uso em produtos de IT e OT (Tecnologia da Operação): a vulnerabilidade batizada de Log4Shell (CVE-2021-44228), descoberta em um componente Java chamado Log4j. A divulgação pública desta vulnerabilidade aconteceu em 09/12/2021 e, poucos dias depois, ela recebeu uma classificação de gravidade CVSS 10 (a mais alta). Nos Estados Unidos, a diretora da Cybersecurity and Infrastructure Security Agency (CISA), Jen Easterly, descreveu a exploração como "uma das mais sérias que já vi em toda a minha carreira, senão a mais séria". No dia 15/12/2021 as tentativas de exploração da vulnerabilidade Log4Shell em sistemas do governo e corporações alcançou um patamar de milhões por dia. Até que os patches fossem disponibilizados pelo desenvolvedor, a Apache, a vulnerabilidade era classificada como um ataque de dia-zero. No entanto, podemos esperar que muitos sistemas permanecem desatualizados e vulneráveis, alongando esta janela de vulnerabilidade. Dentre estes sistemas vulneráveis, certamente, há muitos sistemas de automação.

Este cenário acende uma luz de atenção nos governos – pelo fato de o sistema elétrico ser uma infraestrutura crítica, governos e agências regulatórias têm criado leis e requisitos para a adoção de políticas de segurança cibernética no setor elétrico. No caso do Brasil, o Operador Nacional do Setor Elétrico (ONS), em 1º de julho de 2021, criou a Rotina Operacional (RO) RO-CB.BR.01 - Controles mínimos de segurança cibernética para o Ambiente Regulado Cibernético (ARCiber) e a Agência Nacional de Energia Elétrica (Aneel) publicou a Resolução Normativa Aneel Nº 964, de 14 de dezembro de 2021, que dispõe sobre a política de segurança cibernética a ser adotada pelos agentes do setor de energia elétrica.

Se por um lado as leis e regulamentos dizem o que 'deve' ser feito, os padrões (como a IEC 62443) mostram 'como' fazer. Dada a diversidade de sistemas envolvidos na geração, transmissão, distribuição, comercialização e consumo, a adoção de padrões e normas internacionais garante que todos tenham mecanismos de

controle apropriados e suficientes para evitar e minimizar o impacto e o tempo de recuperação de um ataque cibernético. Os requisitos de segurança cibernética do setor elétrico no Brasil podem ser atendidos usando padrões internacionais, como a ISO/IEC 27019 (Gerenciamento de Segurança), a IEC 62443 (Segurança do Sistema), a IEC 62351 (Segurança na Comunicação) e regulamentos como o ARCiber (Ambiente Regulado Cibernético) no Brasil e o NERC-CIP (Critical Infrastructure Protection) nos Estados Unidos.

Uma política de segurança para redes de IT ou OT tem três pilares comuns e essenciais: pessoas, processos e tecnologia. Ela deve endereçar com a mesma profundidade cada um deles. Em outras palavras, a mera implementação de controles (tecnologia) sem a capacitação dos operadores (pessoas) ou a existência de uma gestão de incidentes (processos) pode resultar em vulnerabilidades que serão exploradas por crackers ('crackers' é o termo mais correto para descrever quem pratica o crime cibernético).

O objetivo deste artigo é explorar os dez principais controles de segurança dos padrões IEC 62443, IEC 62351 e do NERC-CIP para atender aos regulamentos brasileiros do setor elétrico para instalações de automação de energia:

1 - Segmentação da rede e proteção de borda com firewalls;
2 - Controle de acesso e gerenciamento de credenciais;
3 - Registro e monitoramento de segurança;
4 - Hardening do sistema;
5 - Backup e restauração;
6 - Gestão de vulnerabilidades;
7 - Proteção contra malware;
8 - Acesso remoto seguro;
9 - Sistema de Detecção de Intrusão (IDS);
10 - Tratamento de incidentes.

Arquitetura típica de uma subestação

Para iniciarmos a abordagem do artigo é importante o leitor saber que um típico sistema de automação de energia consiste em relés de proteção, controladores de automação de subestação, computadores de interface homem-máquina (IHM), estações de trabalho de engenharia, equipamentos de rede e interfaces de comunicação para diferentes entidades externas. Essas interfaces externas são necessárias para comunicação com centros de controle ou para manutenção remota e para fins de diagnóstico.

A figura a seguir ilustra esta arquitetura e será utilizada como base para discutir uma arquitetura segura. Esta discussão é agnóstica de fabricante ou nível de tensão e pode servir como um modelo inicial para as empresas de energia.

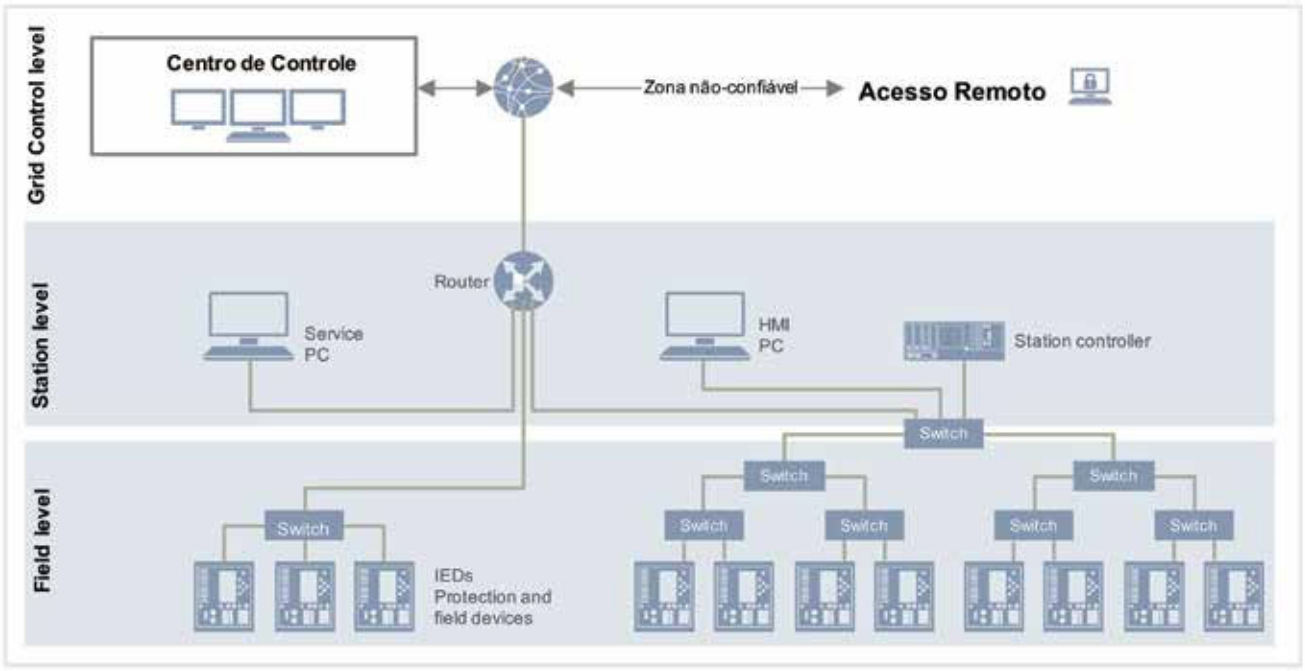

Figura 1 – Arquitetura típica de uma subestação.

Principais direcionadores para subestação segura

No caso do setor elétrico, os principais direcionadores para construir uma subestação segura são ter como guias as normas e padrões internacionais e, mais recentemente, as diretrizes do ONS e da Aneel. Não custa lembrar que as redes de OT prezam pela disponibilidade, integridade e confidencialidade, uma ordem bem diferente das redes de IT.

Rotina Operacional do ARCiber e a REN 964 da Aneel

A Rotina Operacional RO-CB.BR.01 está dividida em seis blocos principais. Cada bloco descreve os controles que devem ser implementados.

- ***Arquitetura:*** segmentação da rede, uso de VPN (Virtual Private Network) e anti-malware;
- ***Governança:*** cria o papel do gestor responsável e a Política de Segurança Cibernética;
- ***Inventário:*** ciclo de 24 meses para inventariar os ativos;
- ***Gestão de vulnerabilidades:*** gestão de vulnerabilidades e atualizações de segurança;
- ***Gestão de acessos:*** gestão de identidades e credenciais privilegiadas;
- ***Monitoramento e resposta a incidente:*** compartilhamento de inteligência, notificação de incidentes e testes dos planos de segurança cibernética.

A Rotina Operacional do ARCiber requer a adoção destes controles apenas nos centros de controle e instalações que se comunicam diretamente com o ONS (além do próprio ONS), enquanto a Resolução Normativa 964 da ANEEL expande a necessidade de adoção de padrões e políticas de segurança para todos os agentes do sistema elétrico e deixa claro que a segurança cibernética das instalações e a continuidade na prestação do serviço são responsabilidades dos agentes. Estes regulamentos determinam o que 'deve' ser feito, mas não detalham 'como' fazer, pois são regulamentos e não padrões normativos e cabe aos agentes definir os controles e as políticas que serão adotados.

A adoção de padrões tem muitas vantagens:

- Abertos;
- Ampla participação das partes interessadas;
- Uniformidade e consistência;
- Estado da arte;
- Relevância internacional;
- Alta aceitação.

Padrões internacionais de segurança cibernética para o setor elétrico

Os principais padrões internacionais para segurança cibernética no setor elétrico são descritos a seguir:

- ***IEC 62443:*** endereça requisitos organizacionais e técnicos para os agentes, para os integradores dos sistemas e para os fornecedores de produtos. Este padrão permite o projeto de soluções de segurança para diferentes finalidades por meio de medidas de segurança de intensidade variável e possibilita a certificação de soluções e processos. A parte IEC 62443-2-4, por exemplo, estabelece requisitos para os fornecedores de sistemas (ex. guias de hardening, que são configurações para reduzir a superfície de ataque) e a parte 3-3 que estabelece controles de segurança para a instalação (ex. segmentação da rede de dados em zonas).
- ***IEC 62351:*** a IEC 62351 aborda a segurança dos protocolos de

comunicação, inclusive a IEC 61850. O foco está na proteção de ponta a ponta, levando em consideração políticas de segurança, processos e tecnologias para impedir efetivamente o acesso não autorizado ou a modificação das informações trocadas. Assim como a IEC 62443, esta norma endereça requisitos para os agentes, para os integradores dos sistemas e para os fornecedores de produtos.

• ***NERC-CIP:*** endereça requisitos apenas aos operadores do sistema e aplica-se aos agentes no Canadá e Estados Unidos, sendo, no entanto, utilizado como referência também em outros países.

Arquitetura da subestação segura

A seguir vamos explorar brevemente como cada um dos controles de segurança é implementado em uma subestação segura. Estes controles têm como base os padrões descritos anteriormente e visam atender aos regulamentos do setor elétrico no Brasil. A Figura 2 apresenta a arquitetura de uma subestação segura, independentemente de fornecedor ou nível de tensão, e pode servir como um modelo inicial.

Segmentação da rede e proteção de borda com firewalls

A segmentação de rede em zonas confiáveis (1) cria barreiras para impedir a propagação de um ataque no sistema. A segmentação deve ser preferencialmente definida durante o projeto e ter pelo menos três zonas:

• ***Zonas seguras ou confiáveis:*** existe pelo menos uma, mas idealmente devem existir mais zonas. Dentro da zona confiável estão todas as funcionalidades de proteção e automação. Esta é uma zona protegida, somente acessível através da DMZ. Adicionalmente, zonas seguras são úteis para proteger dispositivos legados com menos recursos de segurança e, neste caso, restringem ao máximo a conectividade com estes dispositivos (requisito 5.1.1 da RO do ARCiber).

• ***DMZ (Demilitarized Zone ou Zona Desmilitarizada):*** na DMZ ficam os elementos de gerenciamento e que fazem transferências de dados para a zona confiável (logs, patches). Toda a comunicação de entrada e saída é controlada por um firewall.

• ***Zona não-confiável:*** é uma parte exposta da rede (internet ou provedor do serviço de conectividade) e tipicamente separada da DMZ através de firewall.

O requisito para implementar a segmentação está no capítulo 4.1 da Rotina Operacional do ONS, que utiliza o modelo de Purdue como referência. A RO estabelece, pelo menos, três zonas de segurança: zona de Supervisão (nível 2 do modelo Purdue), zona DMZ (nível 3) e zona Corporativa (nível 4), que podem ser feitas fisicamente (diferentes portas) ou logicamente.

Controle de acesso e gerenciamento de credenciais

O controle de acesso (2) é a restrição seletiva de acesso a dispositivos, soluções ou infraestrutura, autenticando usuários (e sistemas) e concedendo as permissões apropriadas. O gerenciamento de credenciais é a definição de diferentes contas de usuário com privilégios adequados, preferencialmente executado de forma centralizada.

O padrão IEC 62351-8 estabelece a base para o controle de acesso, o RBAC (Role Based Access Control – Controle de Acesso baseado em

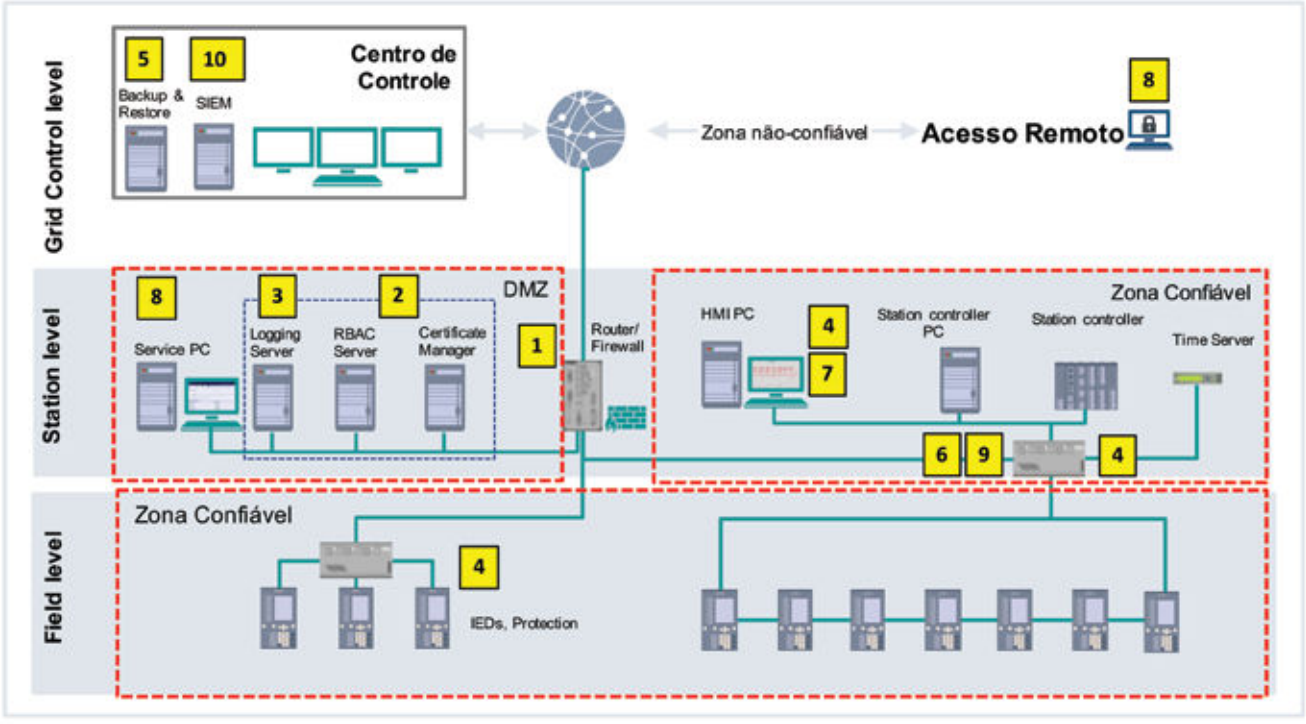

Figura 2 – Arquitetura da subestação segura.

Função), criando associações estáticas entre pessoas, funções, direitos (leitura/ escrita/ administração) e dispositivos. O servidor de RBAC se conecta a um sistema de gestão centralizada e garante a continuidade em caso de distúrbio na comunicação da subestação. Os requisitos de gerenciamento de acesso e credenciais fazem parte do capítulo 4.5 da RO ARCiber.

A autenticação de usuários usando MFA (Muti-Factor Authentication), em que o usuário aplica adicionalmente o código dinâmico de um token ou biometria para se autenticar, tem se mostrado muito importante para prevenir que credenciais roubadas sejam utilizadas. A MFA é citada como uma medida de segurança no capítulo 3 na RO do ARCiber. Uma forma interessante de implementar o MFA para acesso remoto é utilizar este recurso no Firewall que, por sua vez, está integrado ao servidor de RBAC.

A autenticação de dispositivos (estação de engenharia e relés) na rede pode utilizar RADIUS ou Certificados Digitais para criar conexões seguras utilizando TLS/SSL. A vantagem dos certificados digitais é que eles podem ser instalados pelo administrador do sistema em máquinas confiáveis e apenas estas podem se comunicar com os dispositivos (ex. relés).

Registro e monitoramento de segurança

Muitos dispositivos do sistema de automação de energia registram eventos de segurança e atividade (ex. tentativas de autenticação sucessivas) num log de segurança (ex. via Syslog). Estes registros são essenciais para monitorar, detectar e rastrear ataques cibernéticos. Estes logs são enviados para um sistema SIEM (Security Information and Event Management) (10) junto com logs do firewall (1) e do IDS (9) e ficam armazenados em um buffer local em caso de interrupção da comunicação (3).

O tempo de recuperação após uma tentativa de ataque pode ser muito reduzido se o agente conseguir rastrear o ataque identificando as redes e os dispositivos atacados. A RO ARCiber descreve este requisito no capítulo 4.6.1.

Hardening do sistema

O hardening (literalmente 'endurecimento') reduz a superfície de ataque dos produtos e soluções por meio de configuração segura (4) em computadores, switches, relés, etc. Isso é alcançado, por exemplo, pela remoção de software não utilizado, nomes de usuário ou logins desnecessários, desativação de portas não utilizadas ou proteção do sistema operacional. Desabilitar portas não utilizadas de switches, por exemplo, dificulta a conexão de um notebook infectado localmente. A desabilitação de partes de software não utilizadas reduz a capacidade de um cracker explorar vulnerabilidades dele.

O hardening trata apenas de configuração e é idealmente feito durante o projeto e o comissionamento do sistema. Fabricantes e integradores de sistemas devem desenvolver manuais documentando como fazer e documentar todo o hardening feito no projeto. A RO ARCiber descreve este requisito em 4.3.3.

Backup e restauração

O processo de backup e restauração (5) garante que todo o sistema possa ser restaurado depois de uma exclusão acidental ou corrupção dos dados, uma falha de hardware, um ataque de ransomware ou danos nas instalações devido a desastres naturais ou incêndios. O objetivo é restaurar o sistema para o momento anterior ao evento, por isso, dados de todos os dispositivos relevantes devem ser cobertos. O sistema de backup não é descrito explicitamente, mas é a base do plano de resposta e recuperação, conforme capítulo 4.6 da RO ARCiber.

Uma estratégia de backup eficiente começa com quatro perguntas:

- O que? Dados de aplicação, configuração e eventos;
- Quando? Cada tipo de dados muda com frequência diferente e pode estar associado a eventos. A frequência pode ser diária, mensal ou após determinados eventos;
- Como? Sistemas PC podem ter seu backup feito completamente. Já a configuração de dispositivos pode ser copiada através da base de dados de ferramentas de engenharia, por exemplo;
- Onde? Idealmente o backup deve ser feito em uma outra localidade e em um segmento de rede diferente.

Gestão de vulnerabilidades

O gerenciamento de vulnerabilidades de segurança inclui monitoramento de vulnerabilidades em todos os softwares e produtos que compõem um sistema, classificação das vulnerabilidades e patches disponíveis e testes de compatibilidade de patches de segurança.

A base para a gestão de vulnerabilidades é o inventário dos ativos de uma rede (RO ARCiber 4.3), incluindo todo software e hardware. Como as vulnerabilidades em produtos são documentadas em qualquer momento do seu ciclo de vida, este processo deve ser feito com a maior frequência possível. Os fabricantes divulgam em canais públicos as correções para vulnerabilidades em seus produtos, mas os agentes devem monitorar e classificar o risco sistêmico destas vulnerabilidades em seus próprios sistemas e programar as atualizações em janelas de manutenção.

Uma forma eficiente de fazer a gestão de vulnerabilidades é utilizando uma ferramenta de inventário automática, que pode ser instalada em um hardware específico ou dentro de um switch (6).

Os ataques de dia-zero acontecem no período entre a descoberta e a solução pelo fabricante de uma vulnerabilidade. No entanto, muitos ataques exploram vulnerabilidades antigas, fora da janela do dia-zero, devido à falta de um processo de gestão de vulnerabilidades.

Proteção contra malware

A proteção de sistemas baseados em PC é feita por meio de soluções apropriadas de proteção contra malware (7), como antivírus clássico, lista de permissões de aplicativos ou softwares que identificam malwares pelo seu comportamento (assinatura). Tão importante quanto fazer uso desses recursos, é mantê-los atualizados, uma vez que as novas ameaças surgem com frequência cada vez maior. A RO do ARCiber traz este

ENGEREY

PAINÉIS ELÉTRICOS

SOLUÇÃO COMPLETA PARA SUA INSTALAÇÃO ELÉTRICA

EcoXpert LV Panel Certified by Schneider Electric

EcoXpert MV Panel Certified by Schneider Electric

Schneider Electric PrismaSet SM6

SOLUÇÃO COMPLETA PARA SUA INSTALAÇÃO ELÉTRICA

☎ (41) 3022-3050 www.engerey.com.br

requisito no capítulo 4.1.

Particularmente nas redes de automação de energia, dois cuidados devem ser levados em conta: (i) a atualização dos utilitários de anti-malware não podem ser feitos diretamente através da internet e (ii) máquinas com versões antigas de sistema operacional podem não ter suporte a novos malwares e devem ser tratadas como exceção (capítulo 5.1 da RO ARCiber).

Acesso remoto seguro

Acesso remoto seguro no contexto de sistemas de automação de subestações é o acesso criptografado, autenticado e autorizado a ativos de subestação de sites remotos através de potencialmente não confiáveis redes. O acesso remoto apresenta grandes riscos de segurança, se não for adequadamente protegido.

O acesso remoto seguro deve seguir algumas recomendações básicas:

- Deve ser devidamente autenticado, preferencialmente usando MFA;
- O sistema de automação deve prever uma DMZ com firewall próprio, pois o firewall da rede corporativa protege a rede corporativa. Um crescente número de ataques se inicia na rede corporativa e depois migra para a rede operativa;
- O acesso remoto deve ser feito apenas em máquinas específicas, como a estação de engenharia (8), por exemplo, posicionadas na DMZ, evitando o acesso remoto direto a dispositivos como switches ou relés. Este requisito está presente no regulamento do NERC-CIP;
- Ferramentas de acesso remoto que permitem criar logs de atividade devem ser preferidas pois permitem auditar atividades suspeitas.

Sistema de Detecção de Intrusão (IDS)

Sistemas de detecção de intrusão (9) tipicamente monitoram o tráfego de redes industriais em tempo real buscando anomalias que podem estar associadas ou não a assinaturas de ameaças conhecidas. Este tipo de sistema é especialmente útil em redes de automação, que têm um padrão estático de comportamento, ou seja, mudam muito pouco.

As anomalias são alterações no padrão de funcionamento previamente conhecido e podem envolver novos dispositivos conectados, protocolos não utilizados, escaneamento de portas, tentativas de conexão à internet e mudanças no fluxo de comunicação.

Ferramentas de IDS modernas tipicamente ajudam também no inventário de ativos, gestão de vulnerabilidades, auditoria de riscos, mapeamento de fluxos de dados e protocolos industriais em uso.

Tratamento de incidentes

O tratamento de incidentes é o processo pelo qual uma organização lida e reage rapidamente a vulnerabilidades e incidentes, incluindo comunicação interna e externa, conforme requisitos do capítulo 4.4 da RO do ARCiber.

O processo de tratamento de incidentes usa informações dos logs de segurança e da gestão de vulnerabilidades para detectar, responder e recuperar um sistema e deve ser feito da forma mais rápida e segura possível. Um SIEM (10) é uma ferramenta crítica para auxiliar neste trabalho. Um estudo recente da IBM estima em 21 dias o tempo médio de recuperação de um ataque cibernético.

Conclusão e recomendações

O setor elétrico é uma das principais infraestruturas de um país, da qual todas as outras dependem para funcionar, sendo um serviço essencial para a sociedade.

Um ataque de proporções regionais no sistema elétrico pode deixar cidades inteiras no escuro e sem telecomunicações, por exemplo. Além disso, o sistema elétrico é essencialmente ciber-físico e as consequências de um ataque cibernético podem ir muito além da perda de dados ou de receita, colocando em risco a sociedade.

A implementação de uma política de segurança cibernética depende de pessoas, processos e tecnologia. A falta de um destes pilares representa um elo fraco de uma corrente que se quebra com facilidade e desperdiça o trabalho feito nos outros elos. A política de segurança de redes de operação (TO) é essencialmente diferente das redes corporativas (TI) nos seus objetivos e prioridades, mas que devem ter convergência na sua aplicação, monitoramento, execução e resposta a incidentes.

Finalmente, o estímulo regulatório precisa ser visto como um passo apenas, não como um objetivo final. A segurança cibernética precisa ser vista como um pilar para a continuidade do negócio. Assim como a segurança do trabalho foi incorporada à cultura das empresas, a segurança cibernética precisa estar na agenda de todos os líderes do agentes, especialmente os envolvidos na operação do sistema elétrico.

**Rodrigo Leal é graduado e mestre em engenharia elétrica. Possui MBA em Gestão de Projetos pela Fundação Getúlio Vargas (FGV) e curso de Gestão de Negócios da Era Digital pela Cesar School. Atualmente, cursa MBA Executivo de Negócios do Setor Elétrico pela FGV. Desde 2006 atua na Chesf, assessor do Diretor de Operação, coordenando vários processos da diretoria, incluindo os assuntos relativos à tecnologia operativa. Ocupa ainda a posição de vice-presidente do Conselho Diretor da UTC América Latina e Coordenador do Comitê de Tecnologia da Informação e Telecomunicações no Cigre-Brasil.*

Sergio Sevileanu é graduado em Engenharia Elétrica pela UNICAMP e pós-graduado em Administração de Empresas pela Fundação Getúlio Vargas. Tem mais de 20 anos de experiência em desenvolvimento de negócios nos mercados de telecomunicações, energia e infraestrutura, tendo atuado na sede da Siemens na Alemanha. Atualmente é responsável por desenvolvimento de negócios na Siemens com ênfase em conectividade e segurança cibernética. Faz parte das comissões de IoT e segurança cibernética da ABINEE, do grupo de trabalho de 5G do Cigre, membro do comitê de digitalização do Instituto Brasileiro do Petróleo e consultor do Fórum Brasileiro de IoT.