Soluções de Segurança Cibernética para Atendimento ao Submódulo 5.13 do ONS

Eduardo Gonçalves, Vinícius Ferrari e Wesley Roberto

INTRODUÇÃO

A Rotina Operacional RO-CB.BR.01 do Submódulo 5.13, documento publicado pelo Operador Nacional do Sistema (ONS) e intitulado Controles Mínimos de Segurança Cibernética para o Ambiente Regulado Cibernético [1] estabelece os requisitos que devem ser atendidos, neste âmbito, pelos agentes que compõem a rede básica do Sistema Interligado Nacional (SIN).

Os componentes de cada agente abrangidos pelo Submódulo fazem parte do denominado Ambiente Regulado Cibernético (ARCiber), que abrange os centros de operação dos agentes, a infraestrutura sobre a qual são trocadas informações com o centro operativo do ONS ou de outros agentes e o ambiente operativo do ONS. O Submódulo define um conjunto de controles visando aumentar a segurança cibernética do ARCiber.

Esta nota de aplicação descreve soluções utilizando recursos tecnológicos para auxiliar os agentes durante as etapas de implantação e operação dos sistemas em conformidade com as determinações do Submódulo.

INVENTÁRIO DE ATIVOS

A Rotina Operacional define que todos os ativos, softwares e hardwares conectados ao ARCiber devem ser inventariados com uma periodicidade mínima de 24 meses. O inventário deve conter informações acerca do [1]:

- Tipo de dispositivo;
- Fabricante do equipamento;
- Função;
- Endereço IP ou endereço MAC;
- Protocolo de aplicação e/ou porta de serviço;
- Versão do firmware e/ou sistema operacional, quando aplicável.

Embora a elaboração do inventário possa ser realizada de maneira manual, este processo está sujeito a erros e pode ser trabalhoso, tornando-se mais oneroso conforme aumenta-se a quantidade de dispositivos. Neste sentido, ferramentas que possibilitem o inventário de maneira automática diminuem a probabilidade de erros e se adequam à diferentes tamanhos de sistemas.

Dentre as ferramentas automáticas, a SEL possui uma solução baseada nas redes definidas por software (*Software Defined Networks* – SDN), que utiliza as características intrínsecas de segurança proporcionadas por esta tecnologia para a geração eficiente e precisa de relatórios de inventário de ativos. Esta ferramenta é o SEL Flow Auditor.

SEL Flow Auditor

A partir da garantia conferida pela tecnologia SDN de que apenas os fluxos necessários a uma determinada aplicação estão trafegando na rede de comunicação, o aplicativo SEL Flow Auditor é capaz de acessar as configurações dos switches SDN e utilizá-las na geração do relatório de inventário de ativos. A Figura 1 ilustra um exemplo de relatório gerado pelo SEL Flow Auditor. As informações são apresentadas de forma simples, compreendendo os itens requeridos pelo Submódulo e com campos reservados para comentários e anotações.

Device - RTAC

Attributes	Port	Service	Destination (outbound)	Source (inbound)
MAC: 0030A716E556	TCP 443	HTTPS		Laptop
IP: 192.168.1.1	TCP 20000	DNP3	Relay	
VLAN: None	UDP 123	NTP		Relay
Connected to: SW1 port B1	ICMP	Ping	Relay	
	IP	ARP	Relay, Relay IEC61850, Laptop	Relay, Relay IEC 61850, Laptop

Device - Relay

Attributes	Port	Service	Destination (outbound)	Source (inbound)
MAC: 0030A716E430	TCP 23	Telnet		Laptop
IP: 192.168.1.44	TCP 20000	DNP3		RTAC
VLAN: None	UDP 123	NTP	RTAC	
Connected to: SW3 port C2	ICMP	Ping		RTAC
	IP	ARP	RTAC, Laptop	RTAC, Laptop

Device - Relay IEC61850

Attributes	Port	Service	Destination (outbound)	Source (inbound)
MAC: 0030A716E222	TCP 21	FTP		Device 12
MAC: 0030A716E223	TCP 102	MMS		Device 12
IP: 192.168.1.50	TCP 23	Telnet	RTAC	Device 9
VLAN: 100, 200	ICMP	Ping		Device 15
Connected to: SW2 port B3	L2	PTP	RTAC, Laptop	Device 10
and SW3 port C1	L2: VLAN 100	GOOSE	Device 2, 4, 7, 10	
	L2: VLAN 200	SV	Device 3, 6	
	IP	ARP	RTAC, Laptop, SCADA, Relay	RTAC, Laptop, SCADA, Relay

Figura 1 Inventário de ativos gerado pelo SEL Flow Auditor.

O método utilizado para geração do relatório é diferente do utilizado por ferramentas de análise de rede tradicionais, na medida em que a solução com o SEL Flow Auditor não insere nenhum tráfego adicional na rede. Dessa forma, ela não afeta a operação da rede de comunicação, garantindo a manutenção da performance requerida pelas aplicações de infraestruturas críticas para as quais as redes foram projetadas.

MONITORAMENTO E RESPOSTA A INCIDENTES

A Rotina Operacional define que dispositivos de segurança, como firewalls, sistemas de detecção de intrusão (*Intrusion Detection Systems* – IDS), sistemas de prevenção de intrusão (*Intrusion Prevention Systems* – IPS) e subsistemas de autenticação devem ser configurados para gerar alertas no cenário em que identifiquem atividades suspeitas.

Dentre os métodos para monitoramento de redes, a utilização da tecnologia SDN na integração com as ferramentas de monitoramento contribui para melhorar a segurança da aplicação.

Redes SDN e sistemas de monitoramento

Os switches SDN SEL-2740S e SEL-2742S operam com o princípio de negar por padrão, também conhecido como conceito de *whitelist*. Nesta abordagem, são bloqueados quaisquer tráfegos

estranhos à aplicação, sendo permitidos apenas aqueles configurados pelo usuário. Isso representa uma diferença essencial das redes SDN em relação às redes tradicionais, uma vez que os próprios switches realizam o bloqueio de mensagens não previstas.

É possível aproveitar esta segurança proporcionada pela rede SDN e integrá-la a sistemas de monitoramento. A Figura 2 ilustra um exemplo desta integração. Nela, o tráfego de mensagens entre os relés e o concentrador/gateway é permitido pelas regras configuradas nos switches. Porém, em caso de recepção de um pacote estranho, ao invés de simplesmente descartá-lo é possível encaminhá-lo para uma porta específica, à qual está conectada a dispositivos IDS ou IPS, como o SEL UTM, apresentado na próxima sessão. Tais dispositivos podem fazer parte de um sistema de gerenciamento e correlação de eventos de segurança (*Security Information and Event Management* – SIEM), como indicado na figura.

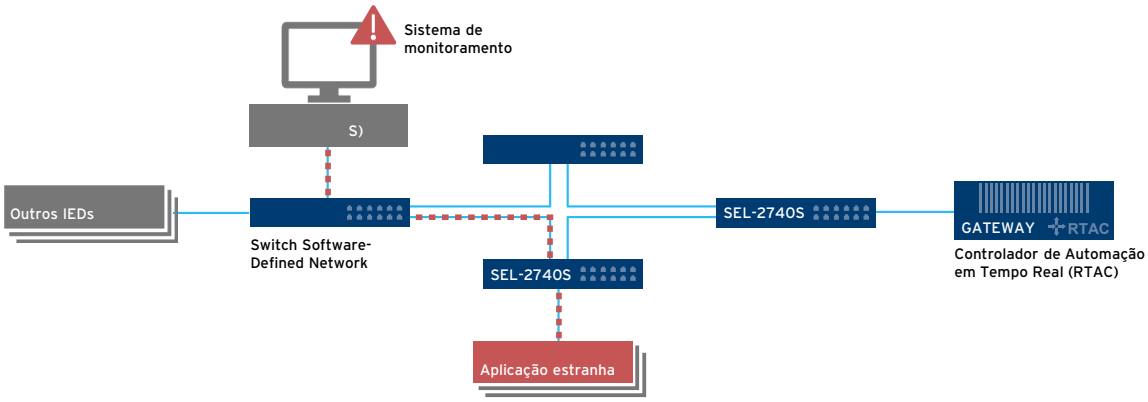

Figura 2 Integração de redes SDN com sistemas de monitoramento.

É importante notar os ganhos de segurança na aplicação do sistema da Figura 2 em relação à utilização de redes com switches convencionais. Nela, o pacote enviado pela aplicação estranha atinge apenas o sistema de monitoramento, de acordo com as configurações programadas nos switches SDN. Em contrapartida, nas redes convencionais este pacote teria possibilidade de atingir quaisquer dispositivos da rede.

ARQUITETURA TECNOLÓGICA ESTABELECIDA

A Rotina Operacional define que as redes devem ser segregadas em zonas de segurança, de acordo com a sua função, que o acesso aos componentes do ARCiber a partir de redes externas deve ser feito por meio de redes privadas virtuais (*Virtual Private Networks* – VPN) e que soluções *antimalware* devem ser implementadas no ARCiber e mantidas atualizadas.

Estas funcionalidades estão disponíveis no dispositivo avançando de segurança cibernética SEL UTM (*Unified Threat Management*).

SEL UTM

A solução SEL UTM integra um firewall de última geração e roteamento avançado no robusto Controlador de Automação SEL-3355, aumentando a resiliência das comunicações entre a rede de subestações e do centro de controle. Esse sistema avançado de segurança cibernética fornece firewall *stateful*, inspeção profunda de pacotes (*Deep Packet Inspection* – DPI), suporte para VPN, roteamento dinâmico e *failover* de hardware.

Todas as funcionalidades são implementadas em sistema operacional fechado, permitindo apenas as aplicações necessárias para o equipamento desempenhar suas funções. Isso contribui para diminuição de vulnerabilidades, na medida em que reduz a superfície de ataque ao dispositivo.

Projetado pelo departamento de Serviços de Cibersegurança da SEL e desenvolvido especificamente para ambientes industriais, o SEL UTM não contém partes móveis e opera em uma ampla faixa de temperatura, de –40° a +75°C.

REFERÊNCIAS

[1] ONS, Submódulo 5.13, Rotina Operacional RO-CB.BR.01, "Controles mínimos de segurança cibernética para o Ambiente Regulado Cibernético", de 2021.