Aprendizados e recomendações

> **Para a prevenção e contenção, MICROSEGMENTAÇÃO! É A REGRA PARA VLANS- PRIVILÉGIO MÍNIMO;**

- Os acessos entre vlans devem ter privilégios mínimos, ao informar apenas a VLAN e definir o acesso como ANY na origem, destino e serviço, você estará liberando o acesso a todo e qualquer serviços e host de uma determinada VLAN para outra;
- Defina exatamente a **Origem (Ip ou grupo pequeno - evite definir uma VLAN) + Serviço + Porta + Protocolo + Destino (Ip ou grupo pequeno - evite definir uma VLAN) exatos;**
  - **EXEMPLO INSEGURO!**

Origem	Destino	Serviço (Porta/Protocolo)	Ação
VLAN1 ou 4.3.2.0/24 ou /16, etc	VLAN2	TODOS (ANY)	LIBERAR (ALLOW)

  - **EXEMPLO SEGURO!**

Origem	Destino	Serviço (Porta/Protocolo)	Ação
4.3.3.0/30 (recepção) Ou IPs individualmente, ou grupos pequenos de IPs	**4.3.2.6 (impressora 1) 4.3.2.7 (impressora 2)**	**JetDirect e PRNREQUEST**	**LIBERAR (ALLOW)**

- Ataques diversos exploram permissões excessivas na rede para um atacante poder se deslocar lateralmente. Para reduzir esse risco, recomendamos:
  - Verificação da segmentação das VLANs.
  - Utilize um host Linux conectado a cada VLAN, uma de cada vez, e execute:

```
sudo nmap -v -Pn -p- --open ip/16+da+rede+interna
```

  - Esse procedimento permite identificar os serviços acessíveis entre VLANs.
    Avalie se os acessos identificados são realmente necessários e ajuste as regras de firewall de rede conforme apropriado.
  -

A cada regra, sempre faça as seguintes perguntas (elas te salvam):

- Preciso de toda essa vlan como origem de tráfego ou apenas algun(s) host(s) dela?
- Este host ou esta vlan de origem, precisa acessar todos os hosts ou todas aquelas vlans de destino?
- Quais serviços essenciais que a origem precisam acessar no destino?!

- **ATENÇÃO TAMBÉM AO CONCEITO DE REGRAS IDA E VOLTA EM FIREWALLS STATEFUL! (armazena o estado de uma sessão/conexão). Se ele permitiu originar uma conexão, ele já sabe que terá volta.**

  - Se o seu firewall opera no modo **stateful**, você não precisa criar regras de volta para o tráfego. Ele armazena o estado das conexões que foram originadas por determinado host e permite que elas sejam retornadas.

ALGUMAS VANTAGENS DO USO DE NGFW em redes (FIREWALL DE PRÓXIMA GERAÇÃO) que fazem diferença neste cenário de incidente:

- **Inspeção profunda de pacotes (DPI):**
  - Com isso a facilidade na detecção de comportamentos anômalos e padrões maliciosos, mesmo que tentem se ocultar;

- **Reconhecimento de aplicativos facilitando bloqueios:**
  - Você não precisará buscar atualizar listas com IPs, portas e protocolos, que podem mudar rapidamente, essas informações são atualizadas automaticamente pelo atualizados automaticamente pelo fornecedor e suas equipes de segurança da solução diariamente, bastando que você aplique as atualizações.
  - **Consulte se é necessária a aquisição de licenças junto ao fornecedor da solução.**

- **Sistema de Prevenção de Intrusão (IPS) e Sistema de Detecção de Intrusão (IDS);**
  - Padrões e regras de detecção atualizados automaticamente pelo fornecedor e suas equipes de segurança, que podem ser aplicados a cada atualização;
  - **Consulte se é necessária a aquisição de licenças junto ao fornecedor da solução.**

- **Integração com inteligência contra ameaças:**

- Você não precisará buscar e atualizar listas com categorias, IPs, portas e protocolos, assinaturas e padrões de tráfego que podem mudar rapidamente, estas informações são atualizados automaticamente pelo fornecedor e suas equipes de segurança, bastando aplicar atualizações.
- **Consulte se é necessária a aquisição de licenças junto ao fornecedor da solução.**

- **Detecção e prevenção de malware:**
  - Informações são atualizados automaticamente pelo fornecedor e suas equipes de segurança, bastando aplicar atualizações.
  - **Consulte se é necessária a aquisição de licenças junto ao fornecedor da solução.**

- **Detecção e prevenção comportamental de tráfego:**
  - Informações são atualizados automaticamente pelo fornecedor e suas equipes de segurança, bastando aplicar atualizações.
  - **Consulte se é necessária a aquisição de licenças junto ao fornecedor da solução.**

- **Proteção contra ameaças avançadas:**
  - Informações são atualizados automaticamente pelo fornecedor e suas equipes de segurança, bastando aplicar atualizações.
  - **Consulte se é necessária a aquisição de licenças junto ao fornecedor da solução.**

Medidas que fazem a diferença na prevenção, tratamento e resposta a esse cenário de incidente:

- **Manter atualizados serviços, sistemas, plataformas e appliances internos.**

- **NÃO utilização de dispositivos não-homologados pela ANATEL:**
  - **Se houver necessidade de experimentos, estes obrigatoriamente devem ser realizados em redes isoladas, sem conexão com outras redes internas e sem conexão com a internet.**

- **Sempre monitore a saúde da sua rede!**
  - **Consumo de recursos, número de conexões, consumo de banda, logs do firewall de borda.**

- **Monitoramento simples e diário da saúde da sua rede, trará excelentes resultados. (top ips de saída, top ip de entrada, consumo de recursos do firewall, número de conexões, revisão periódica das regras, teste entre vlans).**

- **Sempre faça o inventário e a gestão dos seus ativos!**
  - **Você terá a rapidez na resposta a incidentes e informações precisas sob pressão para tomada de decisão e suporte.**

- **OBRIGATORIAMENTE use o MFA em contas técnicas e incentive os usuários a fazerem o mesmo.**
  - **MFA é padrão obrigatório na proteção contra acesssos não autorizados.**

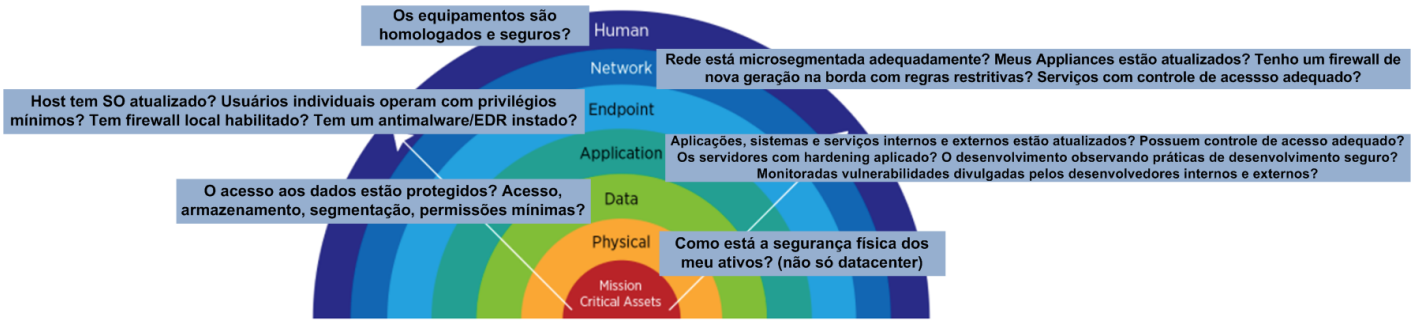
- **Quando for notificado por algum órgão ou entidade ou parceiro, seja por tráfego suspeito, dados expostos, malware, vulnerabilidades ou qualquer outra temática, investigue a causa RAIZ e verifique qual o ativo que é a origem do alerta!**

- **Ao efetuar bloqueios de endereços maliciosos:**
  - **Faça na horizontal (entrada e saída) e na vertical (entre vlans internas).**
    - **DICA: Tenha uma regra de "pânico" pronta para estes momentos (regra vinculada a uma lista de IPs, bastando apenas incluí-los), fácil e rápida.**
  - **É importante esclarecer que esta ação é emergencial e não substitui a identiicação da causa raiz do incidente, é eficaz somente nas primeiras horas de tratamento de incidentes, visto que os indicadores de comprometimento (IoCs) — como IPs, URLs e ASNs — são dinâmicos. Isso significa que o dispositivo comprometido, ao detectar um padrão de bloqueio, pode restabelecer comunicação com o servidor malicioso por novos endereços, tornando bloqueios pontuais ineficazes.**
    - **Assim, sem tratar a causa raiz do comprometimento, a infraestrutura continuará sendo comprometida.**

- **Utilização de solução Network Access Control (NAC) e soluções de postura e autenticação para controle de acesso à rede.**

-

Segurança cibernética deve ser pensada em camadas!



Revision #22
Created 2025-12-08 16:42:39 -03 by Ado Cardoso da Silva
Updated 2025-12-11 12:00:09 -03 by Ado Cardoso da Silva