Medidas e prevenções de ataques cibernéticos

As prevenções em segurança cibernética são essenciais para proteger os ativos da empresa, garantir a continuidade dos negócios, construir confiança com clientes e parceiros, cumprir regulamentações e reduzir custos e danos associados a possíveis ataques.

Veja abaixo alguns métodos de detecção e prevenções de ameaças que a empresa segue para manter sempre um “ambiente” seguro para o sistema.

Firewalls de Rede:

Detecção: Monitore logs de firewall em busca de atividades suspeitas, como tentativas de acesso não autorizado.

Prevenção: Configure o firewall para bloquear tráfego malicioso com base em políticas de segurança.

Antivírus e Antimalware:

Detecção: Realize verificações periódicas em todos os dispositivos para identificar e remover ameaças.

Prevenção: Mantenha os programas antivírus atualizados e configure análises automáticas.

Controle de Acesso:

Detecção: Monitore os registros de acesso para identificar tentativas de login não autorizadas.

Prevenção: Implemente autenticação multifatorial e revise regularmente as permissões de acesso.

Atualizações de Software:

Detecção: Mantenha um inventário de software atualizado para identificar dispositivos ou aplicativos desatualizados.

Prevenção: Automatize as atualizações de software e aplique correções de segurança assim que estiverem disponíveis.

Backup e Recuperação de Dados:

Detecção: Monitore regularmente a integridade dos backups para garantir que os dados possam ser recuperados em caso de ataque.

Prevenção: Implemente backups regulares e armazenamento seguro fora do ambiente principal.

Monitoramento de Tráfego de Rede:

Detecção: Utilize ferramentas de monitoramento de rede para identificar padrões incomuns ou tráfego malicioso.

Prevenção: Configure alertas para atividades suspeitas e implemente políticas de segurança de rede.

Treinamento de Conscientização em Segurança:

Detecção: Avalie regularmente o conhecimento dos funcionários sobre práticas de segurança cibernética.

Prevenção: Realize treinamentos periódicos e simulações de phishing para aumentar a conscientização.

8.Segurança Física:

Detecção: Monitore câmeras e sistemas de segurança física para identificar atividades suspeitas nas instalações.

Prevenção: Limite o acesso físico a áreas críticas e implemente controles de entrada/saída.

Criptografia de Dados:

Detecção: Monitore o uso de criptografia para garantir que dados sensíveis estejam protegidos.

Prevenção: Utilize algoritmos de criptografia robustos e políticas de gerenciamento de chaves eficazes.

Gestão de Vulnerabilidades:

- Detecção: Realize testes de vulnerabilidade regularmente para identificar pontos fracos na infraestrutura.

Prevenção: Priorize e corrija as vulnerabilidades identificadas antes que sejam exploradas por atacantes.

Ao implementar essas medidas e seguir os passos sugeridos para detecção e prevenção, a empresa estará mais bem preparada para lidar com diferentes tipos de ataques cibernéticos.