A tecnologia da Informação na Saúde.

- Segurança da Informação.

Sadraque Cunha

9 de Novembro de 2017

Segurança da Informação na Saúde, por quê?

As Tendências:

- O sector de saúde está mover-se para um modelo mais distribuído:
  - Sistemas de gestão hospitalares interconectados (hospitais, clínicas, laboratórios e centros de atendimento);
  - Enfermeiros, médicos e clínicos precisam ter acesso aos dados do paciente independentemente de onde eles estejam ou que dispositivo usam;

- Internet das Coisas Médicas (IoMT – Internet of Medical Things);
  - Dispositivos médicos e aplicações conectam-se aos sistemas de TI de saúde através de redes de computadores.
  - Monitoramento remoto de pacientes
  - Localização de pacientes internados em hospitais;
  - Dispositivos wearable dos pacientes
  - As Bomba de Perfusão que se conectam a painéis analíticos
  - Camas hospitalares equipadas com sensores que medem os sinais vitais dos pacientes

Segurança da Informação na Saúde, por quê?

A realidade:

- As tendências de TI na saúde aumentam o risco de cyber ataques tal como nunca antes.
  - Quanto maior a quantidade e acessibilidade à informação, maior o interesse por parte de cyber-criminosos;
  - Quanto maior o uso de IoMT maior o número de alvos, maior número de vulnerabilidades e maior o risco.
- Algumas instituições do sector de saúde tendem a cair na armadilha de pensar que são muito insignificantes para serem alvo de ciber-criminosos.
- Os ciber-criminosos vêm esses canais abertos como apenas um outro caminho para o roubo de dados, lucro e controle.
- A segurança comprometida pode interromper funções críticas, interferir com a capacidade de um clínico para tratar pacientes, arriscar a perda de vidas e arruinar a reputação de uma organização.

Segurança da Informação na Saúde, por quê?

As ameaças:

- Dos funcionários
  - Não intencional
  - Intencional

- De rede
  - Packet Sniffers
  - IP Spoofing
  - Defacing
  - Denial of Service (DoS)
  - Spam
  - Man-in-the-Middle Attack
  - Viruses, Trojan Horses, and Worms
  - HTTP Exploits
  - Application Layer Attacks
  - Ransomware
  - Advanced Persistent Threat

O modelo de segurança:

- O modelo de segurança deve permitir fornecer proteção antes, durante e após um ataque.
- Existem três categorias principais de criação de um modelo de segurança:
  1. Criação de uma política de segurança
  2. Monitoramento contínuo e revisão da política de segurança da organização.
  3. Implementação de novos módulos de segurança como indicado por suas necessidades de rede e políticas de segurança.

A Política de Segurança:

- Política de segurança é um documento formal e publicável que define papéis, responsabilidades, uso aceitável e práticas de segurança para a organização.
- Uma boa política de segurança aborda todos os requisitos para proteger pessoas, processos, dados e tecnologia.
- Elementos da Política de segurança:
  - Declaração de Política
  - Escopo
  - Papéis e responsabilidades
  - Diretrizes de segurança
  - Política de Uso Aceitável (AUP)
  - Procedimentos de Resposta a Incidentes
  - Fatores de controle de documentos

As Ferramentas de segurança de rede:

- Soluções de Acesso e Controle de Políticas
- Firewalls de próxima geração
- Sistemas de Detecção de Intrusão de Próxima Geração
- Proteção Avançada de Malware
- Segurança Web
- Segurança de e-mail
- Segurança do DNS
- Assessoria de Segurança, Serviços de Implementação gerenciados

Conclusão

- Planear e implementar uma infraestrutura de rede altamente segura.
- Avaliação cuidadosa de cada área da rede.
- Identificação de potenciais ameaças.
- Desenvolvimento de uma política de segurança.
- Implementação de tecnologias de segurança de rede.

Mayacom – Segurança da Informação

Productos e Serviços:

- Abrangente
- Modular
- Evoluir à medida que as necessidades mudam
- Infraestrutura completa de dados, desde a estação de trabalho, WLAN e o trabalhador remoto e todas as áreas intermediarias.
- Soluções projetadas especificamente para locais de pequeno e médio porte com equipe de TI limitada.
- Conhecimento íntimo das melhores práticas adquiridas com o trabalho em diferentes organizações podendo ajudar os clientes a implementar serviços de rede altamente seguros e com confiança.

4º CONGRESSO
de Ciências da Saúde

MAYACOM