IT Challenges in Healthcare: Scratching the Surface

Mark Boutwell
February 2019

Challenges

- Limited IT resources.
- Legacy and modern IT convergence.
- Fragmented guidance and policy.
- Internal data sharing.
- Voluntary nature of core IT cybersecurity practices in the context of mandated healthcare legislation.

Concerns

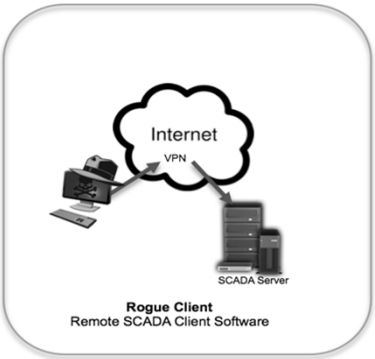
- Unique healthcare IT and data requirements.
- Healthcare data is uniquely linked to the patient, which cannot be easily changed, if at all.
- Policy and governance not operationally flexible.
- Threats keep pace with, or exceed, advances in compliance and security tradecraft.
- Human risks to cybersecurity often overshadow the technical risks, but healthcare challenges rival that of critical infrastructure.
- Vulnerability mitigation will not result in getting out in front of the threat to ensure quick recovery and sustaining services.
- Compliance and security professionals often become a stovepipe tradecraft within the organization.

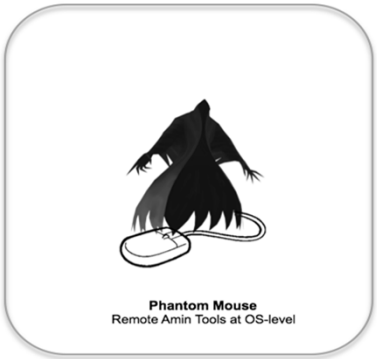
We Are Connected

- Sophisticated social engineering.
- Healthcare IT is easily accessible.
- High profile target considered to be low hanging fruit.
- Data integrity is of primary concern.
- Medical devices are a part of the Internet of Things.

Ukraine Power System Attack

SCADA Hijacking Techniques





The attackers develop two SCADA Hijack approaches (one custom and one agnostic) and successfully used them across different types of SCADA/DMS implementations at three companies

Themes

- Train the workforce to meet compliance and security standards in their daily functions to create a hierarchal tradecraft implementation.
- Traditional compliance and security practices must evolve with active defense practices.
- Insider threats cannot be zero mitigated.
- Capability resiliency is preferred over vulnerability mitigation.
- Compliance and Security cross-pollination are key to awareness and understanding.

Takeaways

- Reality - people and organizations are either the direct target, an enabler, or both.
- Resiliency - vulnerability cannot be zero mitigated; humans and technology are fixed pieces in the threat landscape.
- Strategy - compliance, IT, and training functions must have awareness and understanding of the infrastructure, and of the threats to their collective disciplines.

Considerations

- The way-ahead:
  - IT modernization and policy must sync with compliance, security, and workforce training.
  - Protecting streaming data and data-at-rest (active file system, databases, application access and presentation to the user, etc).
- Implications to:
  - Talent
  - Strategic Planning
  - Modern and Legacy Technology Integration
- Use ingenuity and creativity to overcome today's paradigms to effect positive change.

Closing

Questions and Discussion

Baseline questions (handout) to assist with pattern and behavior analysis.

"It is tough to be strategic when your pants are on fire." – Ron Kifer, VP Global IT, Hewlett Packard