Security Intelligence for Tomorrow's Networks

Wayne Rash
Editor-in-Chief, FierceMobileIT

Peering into the Future

- The greatest weak spot in securing tomorrow’s networks is depending on yesterday’s information.
- Security Information and Event Management tools are useful, but they’re limited and can be unwieldy.
- SIEM only shows what has happened, not what will happen.

Problems in the Past

- Analyzing past event data has uses
  - Alerts to an ongoing attack
  - Traces of penetration attempts
  - Can show what has already failed
- Analyzing past event data has limitations
  - Sorting through false positives
  - The sheer mass of data can overwhelm analysis
  - They can only show existing problems but cannot see the future.

Learning from the Future

- You need to know what will happen next
- The best way to tell what the next threat will be is to see what’s already happening to others.
- Telling the future requires serious research and data from a variety of sources
- Telling what attacks will succeed with your network means you have to really understand your network.

How to Look into the Future

- Know every aspect of every entry point on your network.
  - Everything from USB ports to routers to spam filters.
  - Find ways to control entry points or protect against attacks through those entry points
- Know that you can’t secure everything
  - Plan for failure
  - Know how to detect failure
  - Plan for recovery

What not to do

- Don’t live in the past
  - “We’ve always done it that way.”
  - “It worked last time.”
- Don’t be satisfied with the status quo
- Don’t fail to look for new vulnerabilities
- Don’t underestimate how stupid users can be
- Don’t underestimate how creative your attackers can be

Your Best Plans will Fail

Learn to Recover