

TCP/IP Monitoring

Mark Burnett
Diebold, Inc
Uniontown, OH

- Current TCP/IP service offerings
 - Alarm Monitoring
 - Remote panel programming
 - Video monitoring

- Customer Expectations
 - “Instantaneous” signal transport
 - “Line Security”-Always on connection, will know when there is a problem
 - Alarm Industry is current with newer technology

- Questions to ask
 - Is the customer’s network TCP/IP enabled?
 - Is your network TCP/IP enabled?
 - Are your devices connected via TCP/IP?
 - Does your customer have a network diagram they are willing to share?
 - Who are their network resources?
 - Internal?
 - Outsourced?

- Will you be using a private network connection?
- Public internet connection?
- Hybrid connection?
- If using a private or hybrid connection, who will be responsible for patch management on non-imbedded operating systems?

- Is your customer using an authorized range of IP addresses on their network?
 - Do they own the range of addresses?
 - Are they using hijacked internet addresses?
 - Is there an overlap of addresses between your network and theirs?
- Do they have a resource that performs scans/audits of their network/s for vulnerabilities?

- Transport
 - Frame Relay (Private)
 - Costs more
 - More reliable
 - Less interference
 - Public Internet
 - Lowest cost
 - Intercept of packets possible

- Transport cont.
 - Hybrid
 - Private over customer's LAN, concentrated and transported via public internet
 - Encrypted
 - VPN
 - Two known hosts using internet as transport
 - Encrypted

- Things to watch out for
 - Common exploits
 - Telnet hopping (reassign telnet port or disable if not needed)
 - Unauthenticated logon
 - Use login/password
 - Firewalls
 - Can be closed off during internet worm or denial of service attacks

- Always Always Always have another transmission path, either dial up, cellular or both
- Determine who is responsible for each leg of the network and what steps are to be taken in case of a network outage

- Develop an Interconnection Security Agreement
 - A document that describes why the networks are interconnected, what is permitted across the network and who are the points of contact on both sides, in case of an emergency or problem.