EWIS in a Box

– or –

How to build an national Early Warning System within 80 Days

Jürgen Sander
Dr. Klaus-Peter Kossakowski
Humans are just to slow ...

SAGE (54-65) ... linked hundreds of radar stations in the United States and Canada in the first large-scale computer communications network.

If we would have known earlier ...

.timestamps = {'Humans are just to slow ...': 0, 'SAGE (54-65) ... linked hundreds of radar stations in the United States and Canada in the first large-scale computer communications network.': 230, 'If we would have known earlier ...': 460}
Useful Definition of “Early Warning”

Definition:
- In case of perceptible indicators,
- and (still) a low number of victims, or none,
- information must be distributed,
- to help others – not yet victims,
- including response organisations,
- in order to avoid a major crisis!

Is this possible? Within only 80 days?

- Maybe ... ;)
- It might be that some components are already available
- But there is a lot of confusion and issues around
- Therefore the actual question is better phrased like:

☞ Do you want to be involved!
Existing Indicators are not recognized

- Available indicators
  - New vulnerabilities
  - New attacks
  - New artifacts
  - New patches
- Results depend on human interpretation

üss Realizing trends and potentials!
üss Focused intention on real issues!

Approach
Take a Look at the Challenge

Strategical Dimension
Tactical Dimension
Operational Dimension

And now look from a different Angle

Collecting  Processing  Distributing

Strategical Dimension
Tactical Dimension
Operational Dimension
Objectives

Basic Assumption: CSIRTs are part of the Solution

- Teams already have access to information
  - Creation and improvements of situational reports
  - Trend analysis, comparisons
- Collaboration is supported by the teams
  - Provide access to available information
  - Make use of information that becomes available
  - Together achieve more
Objectives

- **Detection as early as possible**
  - Warnings go out to teams
  - Mitigation and support is coordinated by the teams within their constituency
  - Analysis and coordination is organized among the teams

- **All information must be accessible**
  - Automatic and semi-automatic processing
  - Manual analysis

Target Areas

- **National Security**
  - Information about actual situation
  - Management tool in times of crisis

- **Critical Infrastructure**
  - Information about actual situation – but different level

- **CSIRTs**
  - Support own constituency, including alerting
  - Respond to information regarding their constituency

- **Contributors and Users**
  - Case Studies, Background information
How to create immediate Benefits?

- Visualization and representation of available Information
- Improved Analysis by Humans is key
  - A technical system is “cool” – but does not address all issues
- The technical system needs to support the analysis and provide new functions
  - An analyst is able to prove or disprove her/his hypothesis

---

How to avoid Cascading Effects?

- No closely coupled infrastructures
  - Automatisation is applied for
    - Collection
    - Pre-Processing
    - Internal alerting of analysts
  - External alerting is controlled by humans
    - Approving the “decision” of the technical system
    - Tailored towards the needs of the constituencies
Collecting Data and Information

- **Strategically**
  - Involve all stakeholders
  - Establish governing policies
- **Tactically**
  - Connect existing sources and tools
  - Develop prototypes for missing parts
- **Operationally**
  - Agree on limited number of standards

Provided Data by Partners
Provided Information by Analysts

- While the sensors might be used to get data, information is only provided
  - By humans analyzing available data and providing “the bigger picture” as new entry
  - From other available sources by humans evaluating the information and inserting it
- Harvesting for specific sources might be implemented to some degree
- Aggregation of data might be implemented to generate specific views

Processing Data and Information

- Strategically
  - Support all desired objectives
  - Inline with overall mission and principles
- Tactically
  - Apply existing sources and tools
  - Provide human resources from within the teams
- Operationally
  - Scalability and Availability
Scalability within the Center

CarmentiS: Center - IT-Systems

technical Interfaces, Communication Web, E-Mail, ...

Analyst Workflow and Cooperation Environment

Post-Processing - Aggregation, Correlation,

Storage

Collection and Pre-Processing

---

Distributing Value added Information

- Strategically
  - Serve all stakeholders
  - Establish governing policies

- Tactically
  - Provide easy to use access
  - Provide guidance and user support

- Operationally
  - Provide emergency access in times of an crisis

---

Slide 24 / FISST Conference / ITIS, 29 June 2005
© 2000-2005 by PRESECURE Consulting GmbH
Interfacing with the Center

Wrap Up
Open Issues

- Gaps within the data sources
  - No events reported by partners
  - No events detected by available tools
- Analysis and alert generation needs to be researched in much more detail
- Legal issues
  - Privacy
  - Liability
- Psychology
  - Becoming a „Big Brother“?

Who is alerting whom?

- CSIRTs are already established and are understanding the needs of their constituents,
- Existing communication mechanisms and expertise can be used,
- Providing alerts is in augmentation to their mission and vision

☞ Not every constituency is served!
☞ Alerts might be on different levels!
Early Warning is a Buzzword

- Play it carefully, but make sure, you are involved
- Re-iterate whenever necessary, that there are already teams out there, that are doing it:
  - Collecting and analyzing
  - Warning and alerting
- Understand that others have different goals and might see you as competitor

☞ Make sure you are part of the Solution!

Lessons learned are useful ...

- You can learn from bad experiences of others!
- Someone from the community will suffer, but others will be better of – hopefully :)  
  - which is not really making a difference for the victim site!

☞ If nobody is informing others, nobody else will be safed!
Thus, what enables the wise sovereign and the good general to strike and conquer, and achieve things beyond the reach of ordinary men, is foreknowledge.

Sun Tzu

Thank You!

Contact

Dr. Klaus-Peter Kossakowski

WWW:  https://www.pre-secure.de

Email:  kpk@pre-secure.de
Mobil:  +49 171 5767010