CyTRAP Labs

Roentgenstrasse 49 Street
CH-8005 Zurich Zip Code
Switzerland Country

+41(0)44 272 1876 Voice
+41(0)76 200 7778 Cell

www.CyTRAP.eu/ URL

CyTRAP Labs

An early warning system for home users and SMEs: The ropes to skip

>If we are not careful we will be causing more harm than good

Urs E. Gattiker
CyTRAP Labs & CASEScontact.org

2006-08-31

What is the message?

Our message for today is

> you need to define your market

> running an early warning system is not science

> assessing an incident is neither research nor science, just painstaken technical work
_to get diffusion
_to secure trust and credibility

> you can plan but what happens is another matter all together

> seven hard lessons to be learned – you do not have to repeat our mistakes

Overview

>Infosec
What is our motto

>Set Stage
Characteristics of a successful Early Warning System

>Road to success
What one plans is one thing what happens is often very different

>Raising the bar
The next obstacles we need to manage

>Conclusion
Lessons learned in the process

>Appendix
Additional sources

_Info Sec

The most effective security measures are proactive, not reactive.

If an intrusion or misuse can be detected, then it can also be prevented.

In turn, safer computing encompasses the applying of security patches, and regular auditing.
This means user makes regular self- assessment (or reflection) about security matters and, most importantly, changes his or her behavior accordingly

The above will provide the most protection against the actual effects of security incidents.

But the key is in getting people to do what they know.

_Characteristics of a successful Early Warning System

1. What is the target audience?

2. How should the early warning system be defined?

3. What makes the alerts or guides issued by an early warning system understandable?

4. When should an early warning be issued?

5. What makes an early warning system trustworthy and credible?

_Characteristics of a successful Early Warning System

What is the target audience?

experts (security engineers)
system administrators
media (journalists)
home users (households)
Small and Medium-Sized Enterprises (SMEs)
politicians (public policy decision-makers)
etc.

_Characteristics of a successful Early Warning System

How should the early warning system be defined?

_define the desired message effects or what should recipient do when getting an advisory or a warning, such as:

should they panic?
fix the computer?
get the patch?
stay put?

_Characteristics of a successful Early Warning System

What makes the alerts or guides issued by an early warning system understandable?

clear, precise
what happens if
how to fix the problem
where to get more help

_Characteristics of a successful Early Warning System

When should an early warning be issued?

consistency is the key – Patch Tuesday
sometimes a warning may be issued
(none may be required – but calms nerves)

_Characteristics of a successful Early Warning System

What makes an early warning system trustworthy and credible?

consistent with other sources
public vs. publics (related to target audience issue)
specific
timely
relevant

See more here: What could be the characteristics of a successful Early Warning System?
(http://cytrap.eu/blog/?p=34)

_Road to a successful Early Warning System

1. Target audience

2. Define the early warning system

3. Making alerts or guides understandable

4. Deciding on a system for when to issue an early warning

5. Earning trust and credibility?

_Road to a successful Early Warning System

1. Target audience

Plan home users and SMEs
age group – under 35 years of age
geography Europe, Germany, Switzerland

IS home users, SMEs & sys admin from large organ.
_teachers and school children
15-25 yrs, sys admin up to 60 yrs+, 35-45 years
Europe (DK, NL, B, BU, Slovakia), BRD, CH, Austria,
US, Taiwan, Corea,

_Road to a successful Early Warning System
2. Define the early warning system

Plan issues warnings & alerts
users take action

_Road to a successful Early Warning System

2. Define the early warning system

IS _users visit CASEScongtact.org for the 1/2/3 time(s):

when faced with problem, to get solution:

check security guides and tips,

use checklists, tools, hints on blog.CASEScontact.org

_clicking on links to our content from other:

blogs,

news sites (Taiwan, U.S., Germany)

_subscribe to get customised content via e-mail

html preferred (fewer via RSS)

_Road to a successful Early Warning System
How can we get there?

3. Making alerts or guides understandable

Plan 2 languages, English (see age)
publish on web and via e-mail

2006-08-31

_Road to a successful Early Warning System
How can we get there?

3. Making alerts or guides understandable

IS English alerts,

English (E) & German – step-by-step – fix problem
- _security guides with podcasts
- _blog postings (every 3rd story in German)

podcasts for guides & major security ‚events'
- _iPod – distributed via iTunes
- _directly from our site

Subscribe to get content via e-mail (fewer via RSS)

_Road to a successful Early Warning System
How can we get there?

4. Deciding on a system, when to issue an alert

Plan critical vulnerability and threat with severe impact:
Windows XP,
MS Office & compatible software

IS additionally to the above
_Windows 98,
_show if relevant to MAC or Linux users
_regulation that matters / legal compliance

_Road to a successful Early Warning System
How can we get there?

5. Earning trust and credibility?

Plan subscribers get accurate alerts on time

- email
- RSS

_Road to a successful Early Warning System
How can we get there?

IS we issue alerts warnings as outlined above

++ online glossaries refer to our guides
de.Wikipedia, en.Wikipedia
answer.com, etc.

++ repost/link to blog.CyTRAP.eu or blog.CASEScontact.org
National Assoc. of Local Gov. Auditors mailingList
finance.Google.com
connect.educause.edu – portal for educators
www.lirunning.com – portal for runners / joggers
www.crucesnews.com – news site for city in NM
http://www.kn-online.de/dialog/kn_rss.htm - Kieler Nachrichten

2006-08-31

_Raising the bar
were should we go

_Raising the bar
were should we go

> offer our outputs to other early warning systems

> increase the range of services

> increase penetration and distribution of output

> more servers -- more servers

_Conclusion

What have we learned in this process…

Ropes to skip

2006-08-31

_Conclusion

What have we learned in this process… Ropes to skip

1) Targeting markets	>Its a journey not a destination
2) Value proposition	>What does the user get–is it obvious enough?
3) Give user a choice for content	>html, ASCII, RSS, podcast
4) Being relevant and not too frequent	>what is relevant, find out from your target market

_Conclusion

What have we learned in this process… Ropes to skip

5) Brand CASEScontact.org	>Takes time to secure subscribers‘ trust
6) Serving clients better	>Continuous feedback that must be bundled and applied
7) Finding and exploiting resource advantages	>cost advantage leveraged with market focus

More info here: http://blogs.CyTRAP.eu/?P30

More Info for you

>The above slides have hyperlinks, making it it easy to follow the links to obtain additional information such as, "White papers"

>Additional information can be obtained:

CASEScontact.org
security, virus and threat alerts, tips, weekly newsletter

CyTRAP Labs
better risk management on the way to improved shareholder value - tips, check-lists, white papers

blog.CASEScontact.org-WinCurity
the weblog that helps users improve security with Windows, with freeware, guides and tricks for readers

blog.CyTRAP Labs- EU IST News
the weblog that helps security engineers, system admin personnel and risk managers to achieve better security and assure legal compliance

podscast.CyTRAP Labs radio show
the weblog that allows you to download our podcasts directly or else via different sites such as iTunes

2006-08-31

You can get the slides here:
http://casescontact.org/euist_view.php?newsID=4071

If you need more info, pass me your business card:

>this way you will secure yourself the electronic delivery of the latest version of this presentation and a white paper on this topic in pdf format

>e-mailed to you within 72 hours

CyTRAP Labs

Thanks

Urs E. Gattiker

CyTRAP Labs & CASEScontact.org