Security Service Status in Japan

2008/Feb/28
moto kawasaki
BroadBand Security, Inc.
Market Grows

- Security Services Market Grows
  - 28.1%/yr (2006-2011)
  - ¥105B to ¥363B
- Sec. Products
  - 9.3%/yr
  - ¥279B to ¥436B
- Services surpasses Products?
  - Trend to SaaS/ASP
  - Needs for 3rd party assessment
  - Price Slashing in Product first

Source: Fuji Chimera Research Institute, Inc.
http://www.fcr.co.jp/
Breakdown of Sales est.

• large volume + high growth
  • NW Scan/Pen-Test
  • Managed FW/IDPS
  • Managed Virus Scanner

• Scan/Pen-Test (NW + WebApp) is largest in 2011
  • Let’s dig here.
Annual Growth (%)

- BCP, Timestamp, Online Backup 2007: > 100%, but small in volume
- General Consulting 2008: J-SOX
- NW Scan/Pen-Test: large volume and high growth

Source: Fuji Chimera Research Institute, Inc.
http://www.fcイ.co.jp/
Comparative Market Share

Average Annual Growth

Source: Fuji Chimera Research Institute, Inc.
http://www.fcr.co.jp
NW Scan Industry

• [Demand]
  • large volume + high growth

• [Supply]
  • Better Tools introduced
  • Expensive, but reducing prices

• [New Entrants]
  • Easier entrance for tool-reporter
    • vs. Rare and expensive talented pen-tester

• many new entrants appears

• [Substitution]
  • No major substitution found.
  • Source Code Analysis (SCA)
    • actually, SCA is complement

• [Competition]
  • Demand growth eases a little, but
  • New Entrants slashes prices
  • Severely competing each other
WebApp Scan Ind.

- NW Scan came first, then WebApp
- Almost same situation occurs
- Some conscious demand side
  - Requires 3rd party assessment
  - Places part of Quality Assurance
- Most unconscious ones
  - As Excuse to shirk responsibility
  - “the Cheaper, the better”
5 Forces of Pen-Test Industry in Japan

Bargaining Power of the Suppliers

(-) Better tools introduced
(+-) Expensive tools, but reducing prices
(+++) Rare talented pen-testers

Threat of New Entrants

(+++) Better tools introduced
(++) Easier entrance for tool reporter ==> many new entrants
(--) rare and expensive talented pen-testers
(---) reputation and achievement
(+) MSP/iDC extends its service

Threat of Substitute Services

(-) No Major Substitution
(+-) SCA might be, but actually complemental
(++) in-house pen-tester

Competitive Rivalry within an Industry

(-) Demand growth eases competition
(+) New Entrants slashes prices
(+) Severely competing each other, especially in price
(+++) Rare talented pen-testers

Bargaining Power of the Customers

(-) large volume and high growth
(+)- strong cost-cut demand + many new entrants
(--) required compliance and legal duty

bargaining power of the customers

battle royal to survival war
Current Issue and Measures

• Justification!! for Purchase Order
  • Pay Money requires Result
  • pen-testers won’t guarantee “Never Hacked”
  • FAQ “What actually do I buy, by the way?”

• lack of certification
  • for a web site
  • for an engineer

• desirable grade of pen-test
  • daily/weekly baseline pen-test
  • thorough pen-test quarterly/annual or pre-cutover

• ROI matters
Current Issues

• Justification!! for Purchase Order

• lack of certification
  • for a web site
  • for an engineer

• desirable grade of pen-test
  • daily/weekly baseline pen-test
  • thorough pen-test quarterly/annual or pre-cutover

• ROI matters

• upstream SDLC: Quality Assurance issue
lack of certification

• FAQ “How thorough enough a pen-test should be?”
  • balance between cost and benefit
  • No objective threshold exists
    • One incident may wreck whole efforts

• Needs for common criteria
  • PCIDSS? OWASP top 10? SANS top 20?
  • SANS GIAC WebApp Security? SANS+WASC certification?

• or, Rating and Insurance ?
  • Both services exist but are not famous.
cert. for web site

- requirements
  - list of check points
  - procedure of pen-test
  - criterion of judgement
  - well-known and de facto
- PCIDSS might be a good candidate
  - pros: has first 3 characters
  - cons: too much PCI-focus
- OWASP or SANS top [12]0
  - lack of first 3 items, but famous
cert. for engineers

• requirement
  • rather pragmatic certification
    • like CCIE labo exam
  • covers all area of WebApp and related
  • CPE style of skill updating

• SANS GWAS is a good candidate
  • “SANS GIAC Web Application Security”
  • or SANS+WASC certification to be coming?

• certified engineers validate a web site to be a certified web site
  • ASV/QSA model?
grade of pen-test

• FAQ “How thorough...?” again
  • baseline and deep assessment

• Baseline Pen-Test
  • high frequency: daily or weekly
  • low cost: automatic test
  • low criterion: keep baseline, avoid mis-operation

• Thorough Pen-Test
  • low frequency: quarterly or annual, or at every major release
  • high skill/tool: “certified” pen-tester
    + excellent tools for sufficiency
  • high criterion: check every details to be “certified”
ROI matters

• FAQ “How thorough... ?”
  • Rephrased to “How much money?”
  • Measurement of effect by $$ vs. its cost will persuade top management to purchase.
• Common ROI calculation method?
  • Annual Loss Expectancy vs. Cost
QA Issue: SCA

- Pen-Test traces Attack Vector
- Needs for QA activities, such as SCA
- SCA scans source code
  - no execution of binary object
  - point out flaws, even potential
  - Considered as Quality Assurance issue
    - in the SDLC
    - ex) acceptance test for off shore development

- SCA fixes bugs and improves Quality
  - This may help???
postscript.

• Industry needs to do something to survive
  • in order to escape from battle royal
  • reducing prices really threaten players
  • Grade service levels and Justify the prices!
  • Let Me Survive, Please!!

• Contact
  • moto kawasaki
  • kawasaki@bbsec.co.jp
  • phone: +81 3 5338 7417
  • cell: +81 90 2464 8454