Applicability of ISMS standards in the SME e-commerce sector

Karel Kohout (karel@kohout.se)

Tuesday 7th December, 2010

Definitions

The problem

Applicability of ISMS standards in the SME e-commerce sector?

- SME - Small and medium enterprises
- ISMS - Information security management system, PDCA, controls, objectives[2]
- ISO/IEC 27001 (ISO/IEC 17799)[1]
- Private data protection (95/46/EC)[5][1]

Technical aspects: `http://kohout.se/files/bp.pdf`
Presentation: `http://sorry.vse.cz/~xkohk02/4sa431/pr.pdf`
Paper: `http://sorry.vse.cz/~xkohk02/4sa431/pa.pdf`

[1] "...controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing."[5, Article 17]

Characteristics of SME e-commerce

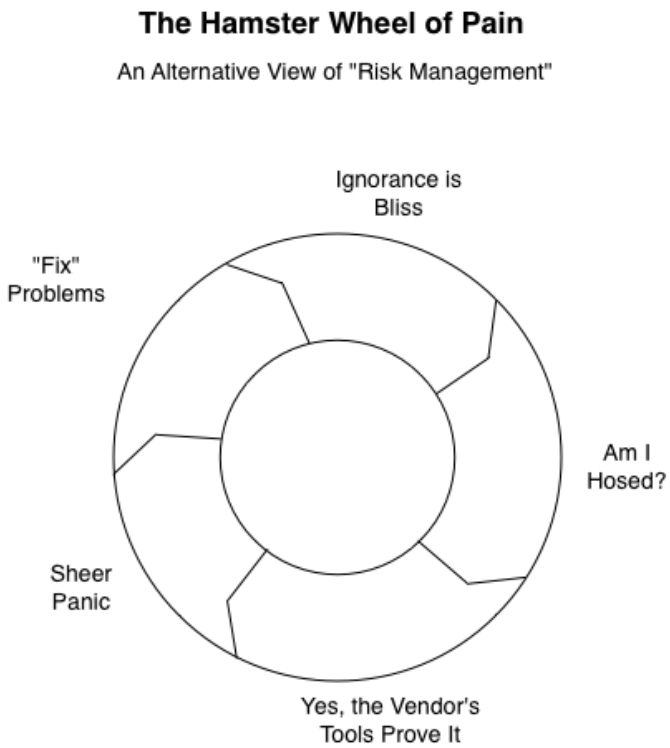
Issues

- Tight budget,
- limited human resources,
- minimal formal policies,
- larger gap between current state and the standard.

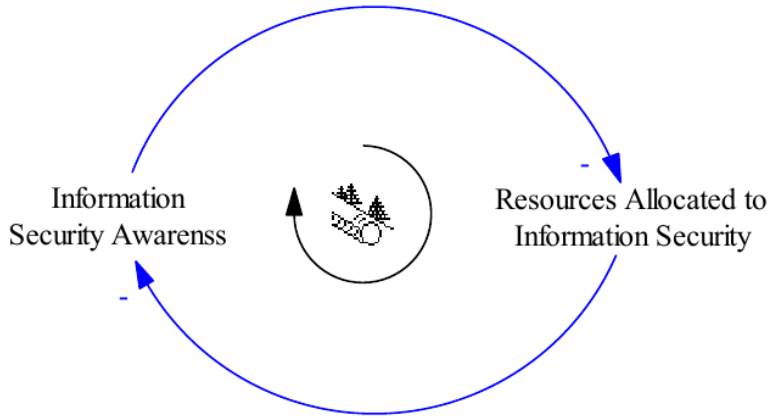
Threats

- Dependence on IS/ICT,
- assets – liabilities,
- extensive legal requirements.

Ad-hoc approach to security



(a) Hamster wheel of pain. Source: [3].



(b) Negative feedback. Source: [4].

Benefits

The System

- Clearly defined responsibilities,
- accountability,
- replaceable employees,
- improvement of processes in other areas.
- Example: domain names.

Improved security, legal compliance

- A.10.9.1: Electronic commerce, A.10.9.2: On-line transactions and A.10.9.3: Publicly available information,
- backups,
- no hidden risks,
- perception of security (selling security to customers).

ISMS issues

Money

- High resource requirements relative to low (perceived) utility.
- Solution: simplification of the framework (NIST[2]).
- Certification, re-cerfitication (broken windows, intermediate system).

Money II (examples)

- Security in third party agreements: SLA[3],
- employee screening,
- ...

[2] National Institute of Standards and Technology

[3] "Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities shall cover all relevant security requirements."[1, A.6.2.3].

The good

security incident = "a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security"[1, 3.6]

The site

- Undisclosed e-commerce site,
- overloaded server,
- outdated server software.

The transfer

- Extensive tests of *business functionality*,
- less than 5 minutes downtime (Sunday around 3 a.m.),
- sanity checks,
- success?

The bad

Monday noon: several thousand emails per minute?

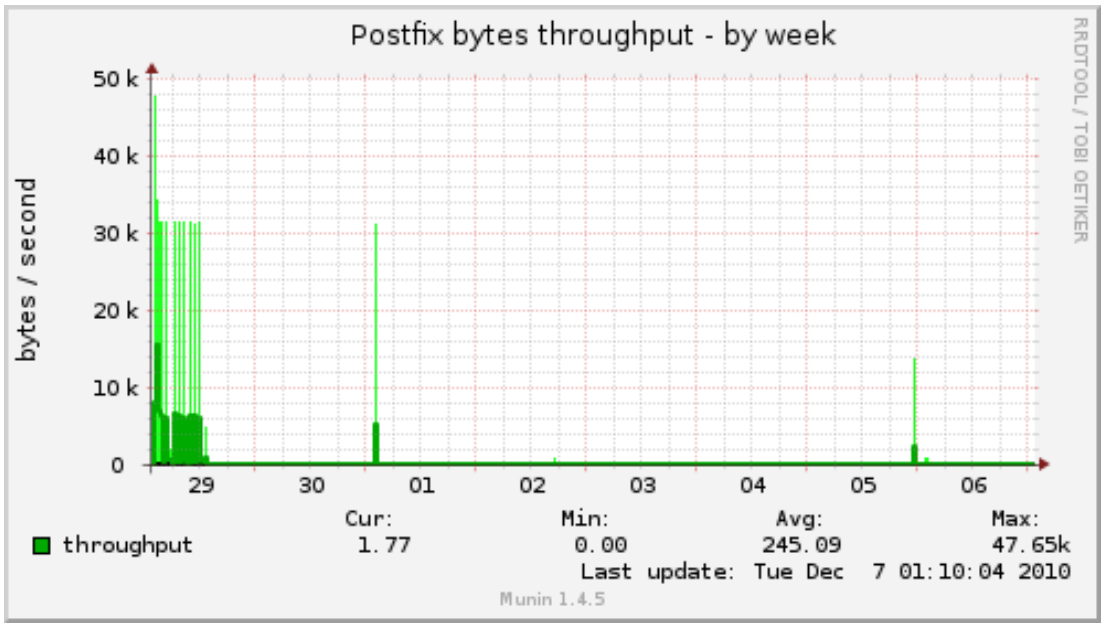


Figure: Postfix (mail transfer agent) throughput, graph from Munin. Source: author.

The ugly

```
...
Nov 29 02:27:22 xyz postfix/smtp[21303]: E018588B3F: to=<Brodkidd@aol.com>, relay=mailin-04.mx.aol.com[205.188.146.194]:25,
 conn_use=3, delay=1.5, delays=0.07/1/0.09/0.28, dsn=5.1.1, status=bounced (host mailin-04.mx.aol.com[205.188.146.194]
 said: 550 5.1.1 <Brodkidd@aol.com>: Recipient address rejected: aol.com (in reply to RCPT TO command))
...
Nov 29 02:27:46 xyz postfix/smtp[21312]: 24FBF88C02: to=<builder4life@aol.com>, relay=mailin-04.mx.aol.com[64.12.138.161]:25,
 delay=6.4, delays=0.06/4.5/1.3/0.59, dsn=4.2.1, status=deferred (host mailin-04.mx.aol.com[64.12.138.161] said: 421 4.2.1
  MSG=:  (DYN:T1)  http://postmaster.info.aol.com/errors/421dynt1.html  (in reply to end of DATA command))
...
Nov 29 02:27:46 xyz postfix/smtp[21339]: 34A8788C04: to=<buildingblks@aol.com>, relay=mailin-02.mx.aol.com[64.12.90.65]:25,
 delay=6.5, delays=0.08/4.4/1.2/0.81, dsn=4.2.1, status=deferred (host mailin-02.mx.aol.com[64.12.90.65] said: 421 4.2.1
MSG=:  (DYN:T1)  http://postmaster.info.aol.com/errors/421dynt1.html  (in reply to end of DATA command))
...
```

421 DYN:T1: “The IP address you are sending from has been temporarily rate limited due to lack of whitelisting, unexpected changes in volume, or poor IP reputation.”

The ugly

Cause

- Tests of “business functionality”,
- minor incompatibility in server software, suppressed exception in CAPTCHA module,
- less than *one day* from vulnerability to discovery and abuse.

Effects

- E-commerce: email delivery critical (order confirmation),
- spam blacklist.

Conclusion

ISMS

- *Business functionality* ('what should work", not security :"what should not be possible"[1, 4.3.1]),
- no clear responsibilities ("Allocation of information security responsibilities")[1, A.6.1.3],
- no formal migration plan[1, A.6.1.4].
- Example: "When operating systems are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security."[1, A.12.5.2]

- Remedy?
- The future.

For Further Reading I


ISO/IEC 17799-2005: Information technology – Security techniques – Code of practice for information security management.. International Organization for Standardization, Geneva, Switzerland. URL: `http://www.iso.org/iso/catalogue_detail?csnumber=39612`.


Doucek, P., Novák, L., Svatá, V., Nedomová, L.: *Řízení bezpečnosti informací*. Professional Publishing, Praha, 2008. ISBN 978-80-86946-88-7.


Jaquith, A., *Security Metrics: Replacing Fear, Uncertainty, and Doubt*. Addison-Wesley Professional, 2007. ISBN 978-0-321-50947-5.


Tawileh A., Hilton J., McIntosh, S., *Managing Information Security in Small and Medium Sized Enterprises: A Holistic Approach*. 2007, ISSE/SECURE 2007 Securing Electronic Business Processes, Part 4, Pages 331-339. URL: `http://www.springerlink.com/content/j938426378g4617k/fulltext.pdf`.

For Further Reading II

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.