Visualizing the Business Impact of Technical Cyber Risks

May 21, 2014
Henk Jonkers
Senior Research Consultant, BiZZdesign
Agenda

• Introduction and problem statement
• Enterprise Architecture with ArchiMate® and TOGAF®
• Enterprise Risk & Security Management with ArchiMate
• Case Study: Pentest-based Business Impact Analysis
• Visualizing the business impact of cyber risks
• Conclusions
Henk Jonkers

- Senior Research Consultant at BiZZdesign
  - Enterprise architecture, ArchiMate and TOGAF
  - Editor of the ArchiMate 2.1 standard
  - Enterprise Risk & Security Management
  - Business Decision Management
- h.jonkers@bizzdesign.com

Case study in collaboration with Bart Seghers, Thales Cyber Security
# Integrated service offering

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Tooling</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Training</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Best practices</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

©BiZZdesign
Customers, offices and partners worldwide

- Netherlands: Enschede, Amersfoort
- North America: Toronto, Boston
- Belgium: Leuven
- UK: London
- Slovakia / Eastern Europe: Bratislava
- France: Paris
- Germany / Central Europe: Düsseldorf
- Sweden / Nordic countries: Stockholm

Partners
- Latin America: Dux Diligens
- Mexico: Unycorp
- Australia: Neodata
- Portugal: Process Sphere
What you will learn today

- How to incorporate risk and security aspects in your EA models
- Combining Enterprise Risk & Security Management with ArchiMate brings risk and security to the boardroom
- How to visualize vulnerabilities of the IT infrastructure in your EA models
- How to achieve more balanced decision making based on risk and security measures
Problem statement

- Organizations are increasingly networked and thus more complex
- Attacks on information systems are becoming increasingly sophisticated
- Attacks use digital, physical and social engineering and the departments responsible for each of these domains within an organization operate in silos
- Current risk management methods cannot handle the resulting complexity
Limitations of current approaches

- Existing information security and risk management methods do not systematically identify potential attacks
  - They are based on, e.g., checklists, heuristics and experience
- Security controls are applied in a bottom-up way
  - They are not based on a thorough analysis of risks and vulnerabilities
  - No explicit definition of security principles and requirements
- Focus on only IT security
  - They have difficulties in dealing with complex attacks on socio-technical systems, combining physical/digital access, and social engineering
- Focus on preventive security controls
  - Corrective and curative controls are not considered
Characteristics of Enterprise Risk & Security Management

- Integral vision on security: protection of business, information, application and technology assets
- Structured identification and analysis of risks and vulnerabilities
- Supports strategic risk management
- Supports “Security by Design”
ENTERPRISE ARCHITECTURE WITH ARCHIMATE® AND TOGAF®
What is Enterprise Architecture?

• **A discipline**, with the objective of **steering changes**
  
• **A product**
  – A design that shows the coherence between products, processes, organisation, information supply and infrastructure, based on a vision and certain explicit starting points, principles and preferences

• **A process**
  – Way of working
  – Aimed at the development and use of enterprise architectures within an enterprise
  – With people and resources
Ingredients for a successful EA practice

TOGAF

Process

Viewpoints

Language

Repository, Reference Models

ArchiMate
The TOGAF Architecture Development Method (ADM)

1. "Getting the organisation committed & involved"
2. "Getting the architecture right"
3. "Making the architecture work"
4. "Keep the process running"
The ArchiMate language

A basis for

High-level modelling within domains

Modeling relationships between domains

Relating detailed design models

Visualizations

Analysis

©BiZZdesign
ArchiMate + TOGAF

Free download of the whitepaper “Enterprise Architecture with TOGAF 9.1 and ArchiMate” here: http://www.bizzdesign.com/downloadmanager/download/293

©BiZZdesign
ENTERPRISE RISK & SECURITY MANAGEMENT WITH ARCHIMATE

©BiZZdesign
Why ArchiMate for Risk & Security Architecture?

- Widely accepted open standard for modeling enterprise architecture
- Tool support widely available
- Good fit with other EA and security frameworks (TOGAF, Zachman, SABSA)
- ArchiMate models integrate business, information, application and technology architecture
- Link with (security) requirements, principles goals (Motivation extension) → Traceability
- Link with detailed design languages for business processes and IT solutions (e.g., BPMN and UML)
- Suitable as a basis for (qualitative and quantitative) analysis and visualization
ArchiMate Risk project

• Collaboration of ArchiMate Forum and Security Forum

• Two areas of concern:
  – Risk analysis
  – Security deployment (risk mitigation)

• Investigate how (specializations of) existing ArchiMate concepts (Core and extensions) can be used

• Inspired on well-established risk and security standards and frameworks, including COSO, FAIR, SABSA

• White paper in progress
Proposal for a “Risk Overlay” for ArchiMate
Proposal for a “Risk Overlay” for ArchiMate
Enterprise Risk Management with ArchiMate

1. Identify threats
2. Analyze vulnerabilities
3. Assess risks
4. Specify required control measures
5. Implement control measures
6. Execute & monitor
CASE STUDY: PENTEST-BASED BUSINESS IMPACT ANALYSIS
Case study partners

BiZZdesign


THALES

- Cyber security consultancy, solutions and services
- Pentesting and Pentest-based BIA
What is a pentest?

- **Goal pentest:**
  - Find weak spots and threats in a network infrastructure and/or a web application
  - Advise on ways to fix and mitigate these weak spots and threats

- **Pentesting from different perspectives:**
  - External: “what can a hacker (ab)use or do from the internet?”
  - Internal: “what can a hacker or employee do when he/she is in your network?”
Pentest approach

- Partly automated (vulnerability scan)
- Human interpretation and customized advice
Automated vulnerability scans

<table>
<thead>
<tr>
<th>Plugin ID,CVE,CVSS,Risk,Host,Protocol,Port,Name,Synopsis,Description,Solution,See Also,Plugin Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;10028&quot;,&quot;,&quot;&quot;,&quot;None&quot;,&quot;192.168.1.1&quot;,&quot;udp&quot;,&quot;53&quot;,&quot;DNS Server BIND version Directive Remote Version Disclosure&quot;,&quot;It is possible to obtain the version number of the remote DNS server.&quot;,&quot;The remote host is running BIND or another DNS server that reports its version number when it receives a special request, for the text 'version.bind' in the domain 'chaos'. This version is not necessarily accurate and could even be forged, as some DNS servers send the information based on a configuration file.&quot;,&quot;It is possible to hide the version number of bind by using the 'version' directive in the 'options' section in named.conf&quot;,&quot;The version of the remote DNS server is: PowerDNS Recursor 3.3 $Id: pdns_recursor.cc 1712 2010-09-11 13:40:03Z ahu &quot;$</td>
</tr>
</tbody>
</table>

"10107",","","None","192.168.1.1","tcp","9999","HTTP Server Type and Version","A web server is running on the remote host.","This plugin attempts to determine the type and version of the remote web server.","n/a","The remote web server type is: Router Webserver" |

"10287",","","None","192.168.1.1","udp","0","Traceroute Information","It was possible to obtain traceroute information. A makes a traceroute to the remote host.","n/a","For your information, here is the traceroute from 192.168.1.101 to 192.168.1.1: 192.168.1.101192.168.1.1" |

"10386",",","None","192.168.1.1","tcp","80","Web Server No 404 Error Code Check","The remote web server does not return 404 error codes.","The remote web server is configured such that it does not return '404 Not Found' error codes when a non-existent file is requested, perhaps the victim instead a site map, search page or authentication page. Nessus has enabled some countermeasures for this. However, they might be insufficient. If a great number of security holes are reproduced for this port, they might not all be accurate.","n/a","CGI scanning will be disabled for this host because the host responds to requests for non-existent URLs with HTTP code 301 rather than 404. The requested URL was: http://192.168.1.1/VSyR5y2HeYUt.html" |

"10386",","","None","192.168.1.1","tcp","9999","Web Server No 404 Error Code Check","The remote web server does not return 404 error codes.","The remote web server is configured such that it does not return '404 Not Found' error codes when a non-existent file is requested, perhaps the victim instead a site map, search page or authentication page. Nessus has enabled some countermeasures for this. However, they might be insufficient. If a great number of security holes are reproduced for this port, they might not all be accurate."
20007 (19) - SSL Version 2 (v2) Protocol Detection

Synopsis
The remote service encrypts traffic using a protocol with known weaknesses.

Description
The remote service accepts connections encrypted using SSL 2.0, which reportedly suffers from several cryptographic flaws to conduct man-in-the-middle attacks or decrypt communications between the affected service and clients.

See Also

Solution
Consult the application’s documentation to disable SSL 2.0 and use SSL 3.0 or TLS 1.0 instead.

Risk Factor
Medium

CVSS Base Score
5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

Plugin Information:
Publication date: 2005/10/12, Modification date: 2011/03/11

Hosts
10.100.1.10 (tcp/636)
10.100.1.10 (tcp/3269)
10.100.1.11 (tcp/636)
Details of a vulnerability

The remote service accepts connections encrypted using SSL 2.0, which reportedly suffers from several cryptographic flaws and has been deprecated for several years. An attacker may be able to exploit these issues to conduct man-in-the-middle attacks or decrypt communications between the affected service and clients.
Host perspective

- Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
  - Terminal Services Encryption Level is not FIPS-140 Compliant
  - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits (69551)
  - tcp/3389
  - tcp/443
  - tcp/5050

- Vulnerability in Microsoft SQL Server Could Allow Remote Code Execution
  - Application server (192.168.1.123)

- SSL Version 2 (v2) Protocol Detection

Legend:
- 0. No risk
- 1. Low
- 2. Medium
- 3. High
Option 1 – configuration from EA

1. Use the enterprise architecture to set the scope of the pentest
   - Top-down analysis
2. Perform a focused pentest
3. Import and analyze results in EA model
   - Bottom-up analysis
   - Insight in risks to (critical) business processes
Option 2 – Manual configuration

1. Perform pentest or use results from a previously performed pentest

2. Create Enterprise Architecture
   - Possibly partly automated, based on pentest results

3. Import and analyze pentest results in the EA model
   - Bottom-up analysis
   - Insight in risks to (critical) business processes

(1) Create EA model
(2) Top-down analysis
(3) Set scope of pentest
(4) Perform pentest
(5) Import / interpret pentest results
(6) Bottom-up analysis ("business impact")
(7) Visualisation of business impact
Top-down analysis
Perform pentest
Bottom-up analysis

Business Layer

- Request received
  - Intake
  - Assess request
  - Pay
  - Notify requester
  - Reject request

Application Layer

- CRM application
- Financial application
- Database application
- E-mail-client

Technology Layer

- Application server (192.168.1.123)
- Database server (192.168.1.101)
- Client PC (192.168.1.188)
## Business impact of technical risks

### Example: Missing critical patches on Database Server

<table>
<thead>
<tr>
<th>VA – 01</th>
<th>Missing critical patches which can lead to jeopardization of the server</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Technical risk</td>
</tr>
<tr>
<td></td>
<td>High</td>
</tr>
<tr>
<td>Present on system(s)</td>
<td>192.168.1.101 (Database Server)</td>
</tr>
</tbody>
</table>

### Description

This system misses critical patches for the Microsoft Operating System concerning the following security bulletins:
- MS08-067: Conficker patch – Published in 2008
- MS06-040: Published in 2006

This leads to multiple weaknesses on the system. Exploiting these weaknesses can lead to:
- Running own/arbitrary code on the system
- Buffer overflow in the server service which may put the system in jeopardy

### Recommendation

Install missing patches

### Impact on Business

Business processes “Intake” and “Notify requester” depend on this Database Server and are the processes that “fill” this server with (sensitive) data. When this server is compromised by exploitation of abovementioned vulnerabilities, then the attacker can steal personal data from the registering applicants as well as modify who will be informed on its registration request.

### Business risk

Medium

### Business recommendation

Because of the low effort necessary to process the (technical) recommendation in combination with the Medium business risk, we recommend to process the technical recommendation within 1 month.
Summary of a pentest-based BIA
VISUALIZING THE BUSINESS IMPACT OF CYBER RISKS
Risk analysis

- Unauthorized access to payment data
- Unauthorized access to request data
- Prevent unauthorized access to confidential data
- Disable SSL 2.0, use SSL 3.0 or higher instead.

Business Layer:
- Handle request
- Intake
- Assess request
- Pay
- Notify requester
- Reject request

Application Layer:
- CRM application
- Financial application
- Database application
- E-mail client

Technology Layer:
- Application server (192.168.1.123)
- Database server (192.168.1.101)
- Client PC (192.168.1.188)

SSL Version 2 (v2) Protocol Detection

Interception of confidential data
Man-in-the-middle attack
Example visualization: Risk factor versus process criticality

Risk factor versus process criticality

- Acceptable
- Acceptable with mitigation
- Unacceptable

Legend:
- Pav
- Reject request
- Intake
- Assess request
- Notify requester
Example visualization: Confidentiality, Availability and Integrity
CONCLUSIONS

DRAW YOUR OWN CONCLUSIONS !!!
A pentest-based BIA:

- Makes the business impact as a result of cyber risks visible and measurable
- Powerful management dashboard
- Facilitates focused testing of technical components supporting critical business processes
- Provides insight in the business risk when adding new components to your technical infrastructure
- Increases the return on investment for your enterprise architecture effort
Summary

• Current risk management approaches, working in isolation, fall short in the complexity of current organizations

• A model-based approach for Enterprise Risk & Security Management is needed
  – Systematic analysis of threats and vulnerabilities
  – Integrated design of control measures

• The ArchiMate language provides the hooks for integrated risk & security modeling, integrated with Enterprise Architecture

• EA models support business impact analysis of technical risks / vulnerabilities
Integrated tool suite

- **Architecture Tools**
  - Design, communicate & analyze architectures
  - Incorporating risk & security aspects
  - Easy to use
  - Integrated in one repository
Consultancy on Enterprise Architecture and Enterprise Risk & Security Management

• Integrated consultancy
  – Workshops and consultancy services
  – Kick-start your EA or Enterprise Risk & Security Management initiative
  – Implementing TOGAF, ArchiMate, Enterprise Risk & Security Management
Training on Enterprise Architecture

- ArchiMate & Architect training, 3 days (open/in house)
  - ArchiMate language
  - BiZZdesign Architect
  - Includes ArchiMate certification

- TOGAF certified training, 4 days (open/in house)
  - Foundation 2 days, Practitioner 2 days
  - Includes TOGAF certification

- Security architecture training, 1 day
  - Modelling a security architecture with ArchiMate
Contact info and more information
A copy of these slides: www.bizzdesign.com/downloads and select “webinars”

blog.bizzdesign.com


- Free trial version: www.bizzdesign.com/tools/bizzdesign-architect/
- Whitepaper EA with ArchiMate® and TOGAF ®: http://www.bizzdesign.com/downloadmanager/download/293

The Open Group

- Downloadable versions of the full specifications of ArchiMate and TOGAF at http://www.opengroup.org
- Many whitepapers, and recorded webinars

BiZZdesign

- General information about BiZZdesign: http://www.bizzdesign.com
- The website of our Academy: http://www.bizzdesign.com/training
- Our Tool, BiZZdesign Architect http://bizzdesign.com/tools/bizzdesign-architect/