»|secaron

Managing Business Risks provoked by Security Threats

Laurent Mellinger
CTO

e.security solutions

Agenda

»|secaron

- What is IT security ?
- The security management process
- Security management and ITIL synergies

The Three Fundamental Principles

»|secaron

- IT security consists in the preservation of data
  - Confidentiality
  - Integrity
  - Availability

Confidentiality

»|secaron

- **Ensuring information is accessible only to those authorised**

- Theft of credit card details
- Email communications interception
- Password sniffing

Integrity

»|secaron

- **Ensuring the accuracy and completeness of information**

- Change articles unit price on an e-commerce platform
- Modify an employee salary amount

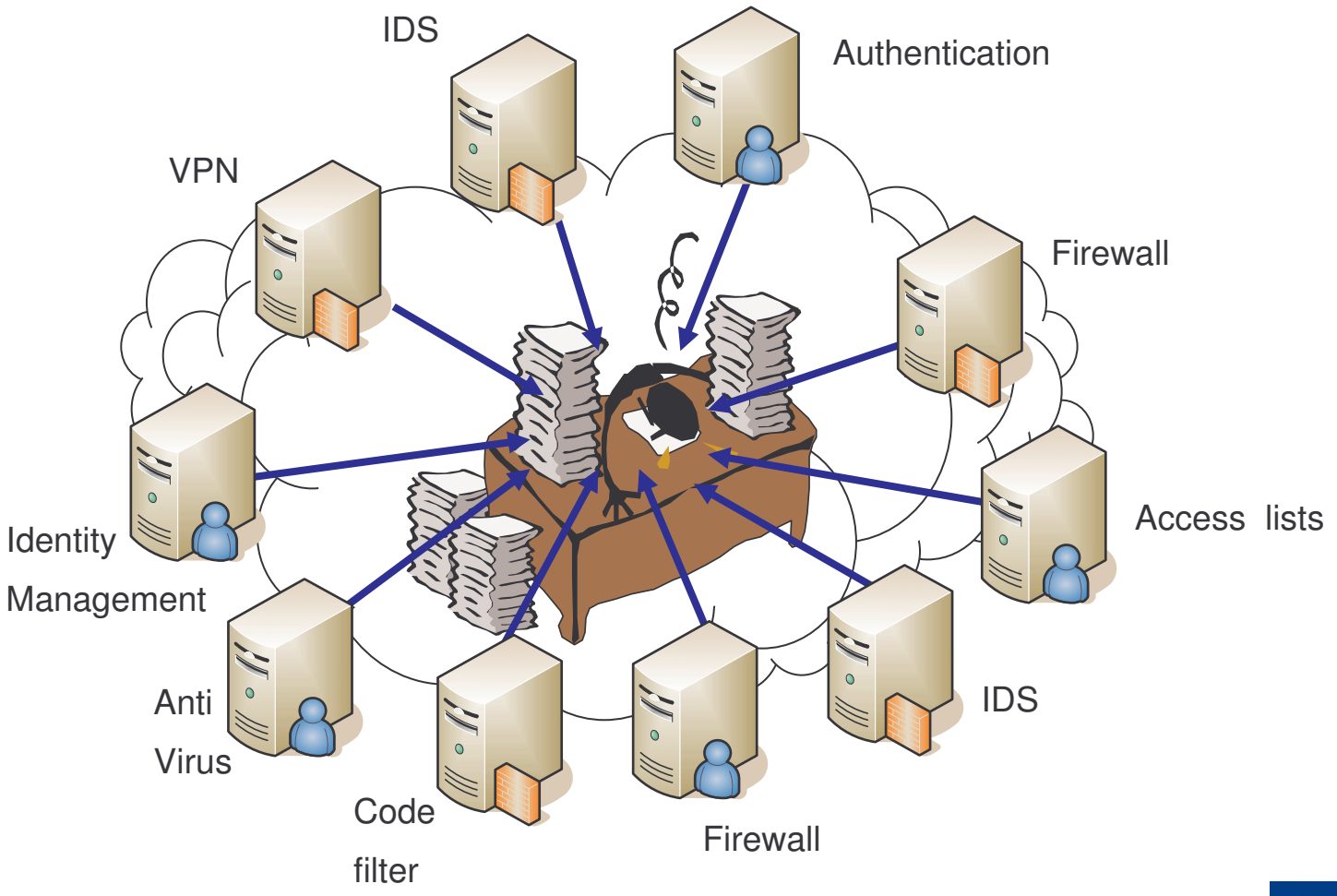
Availability

»|secaron

- **Authorised users have access to information when required**

- Malicious code takes network down
- Distributed Denial of Service attack
- Database corruption

The Initial Goal : Prevent

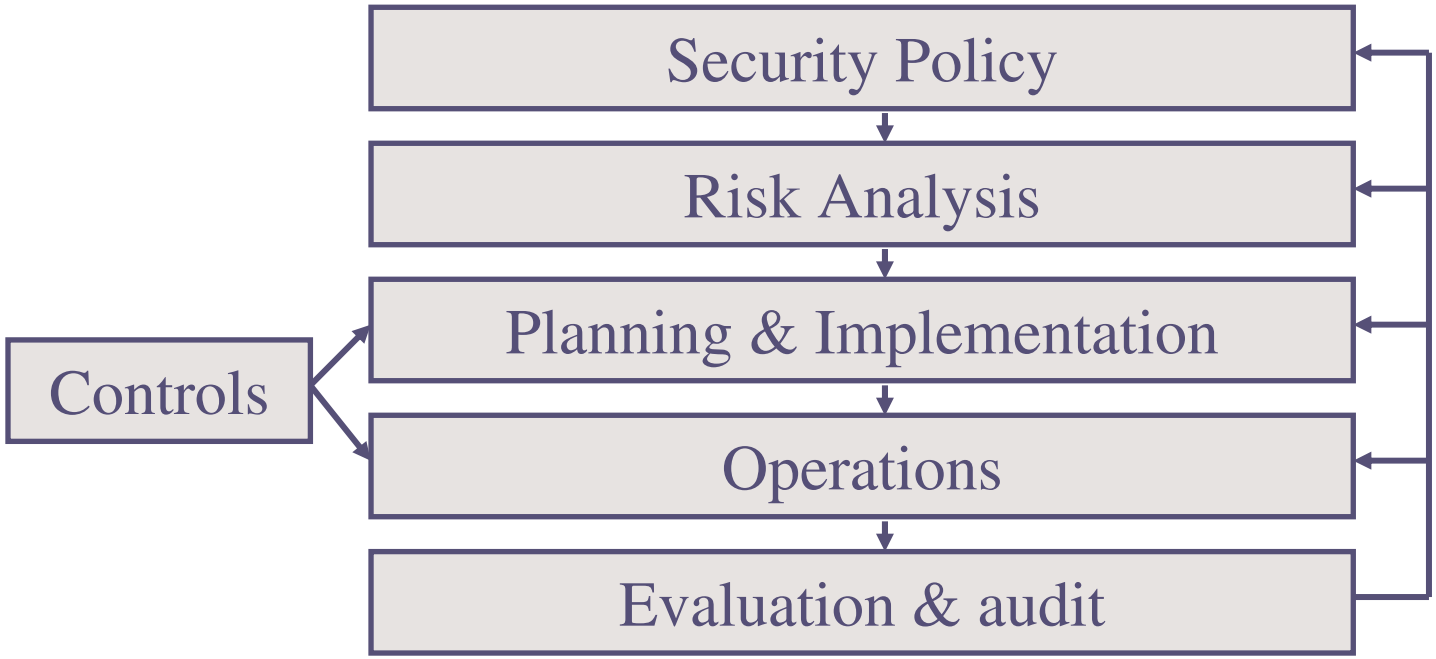


Usual Questions

»|secaron

- Which version of the firewall do we run ?
- Who did update the IDS with the latest signatures and when was it ?
- Is our web server vulnerable to the new worm discovered this week-end ?
- Does it make sense to buy an application firewall ?
- What should I do if our web banking platform gets compromised ?

Security Management



Security Policy

»|secaron

- Synthesis of best practices in terms of security
- Defines a global framework regarding security in the enterprise
- Balance between productivity and security
- Must have top management strong support
- Valid for everybody in the company
- Must state what happens in case of non respect

- Is of no use if :
  - Not distributed across the enterprise
  - Its application is not controlled

Risk Analysis

»|secaron

- Probability that threats exploit vulnerabilities, inducing loss
- Risk = Threat x Vulnerability
- Quantitative approach
  - AV x EF = SLE
    - AV: asset value, EF: exposure factor, SLE: single loss expectancy
  - SLE x ARO = ALE
    - ARO: annualized rate occurence, ALE: annualized loss expectancy

Controls

»|secaron

- Goal : Put controls in place in order to bring risk to an acceptable level, as defined by the security policy

- Organisational measures
  - Incident response, operational procedures, user awareness…
- Technical
  - Authentication, access control, encryption…

Evaluation & Audit

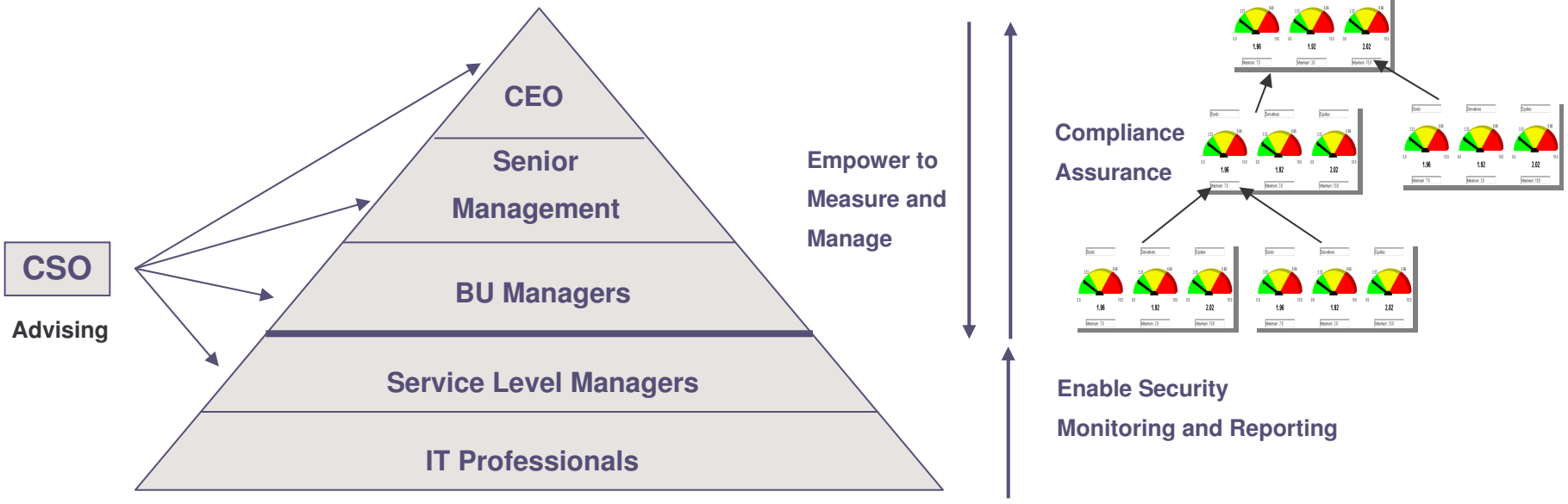
»|secaron

- Goal : Check that existing controls produce expected results

- Organisational
  - Operational procedures review, user awareness evaluation…
- Technical
  - System, network and application audit
  - Penetration tests
  - Source code audit

Motivations

The Players


CEO
Senior Management
BU Managers
Service Level Managers
IT Professionals
CSO
Advising
Empower to Measure and Manage
Compliance Assurance
Enable Security Monitoring and Reporting

»|secaron

Service Support / Security Management Integration

Service Desk

»|secaron

- Security “FrontOffice”
  - Service desk should be able to identify security issues in requests, classify and track them
  - Escalate security issues if necessary
  - Identify malware propagations
  - Consolidate data in order to adapt security management
  - User awareness opportunity
- User and profile management

Incident Management

»|secaron

- Integration of the security monitoring in the ITIL incident management process
- Security incident response could be a sub-part of ITIL incident management
- Integrate forensics analysis into incident management to address the conflict between service availability and incident analysis

Problem Management

»|secaron

- Vulnerability management should be part of ITIL problem management
- Compliance issues should be considered as problems in order to be tracked, and subject to reporting

Change Management

»|secaron

- Security management can initiate changes (technical or organisational)
- Security management can be affected by changes in others processes
- Security management should have an impact in any change request

Release Management

»|secaron

- Security should be introduced in the release management process from the beginning on, to avoid being the blocking element at the end of the process
- Security management should clearly define CIA requirements for any project and introduce them in the release management process
- Security products and patch management could also be managed within the release management process

Configuration Management

»|secaron

- Each configuration item could be assigned a risk rating in order to facilitate security management

ITIL and Security Management

»|secaron

- Minimise costs through tight integration of security, quality and service management
- Achieve efficiency through early consideration of security elements already in concept, planning and operation of IT services
- Creation of well defined interfaces for customers and partners
- Provide measurable IT services
- Enlight links between business needs, IT processes and infrastructure usage
- Consequent planning and operation of IT services regarding security, quality and efficiency
- Costs for IT security are often seen as general fix costs. The possibility to assign costs to concrete processes allow to distribute the spent amount to specific cost centers

Contact Us

secaron S.à r.l.
12, route du Vin
L-6794 Grevenmacher

Luxembourg
Phone: +352 267 469 30
Fax: +352 267 469 32
info@secaron.lu
www.secaron.lu

secaron AG
Ludwigstrasse 55
85399 Hallbergmoos
Near Munich airport
Germany
Phone: +49 811 95 94 – 0
Fax: +49 811 95 94 – 220
info@secaron.com
www.secaron.com

e.security solutions