IBM Globalne storitve

Linux in varnost

Borut Žnidar, borut.znidar@si.ibm.com

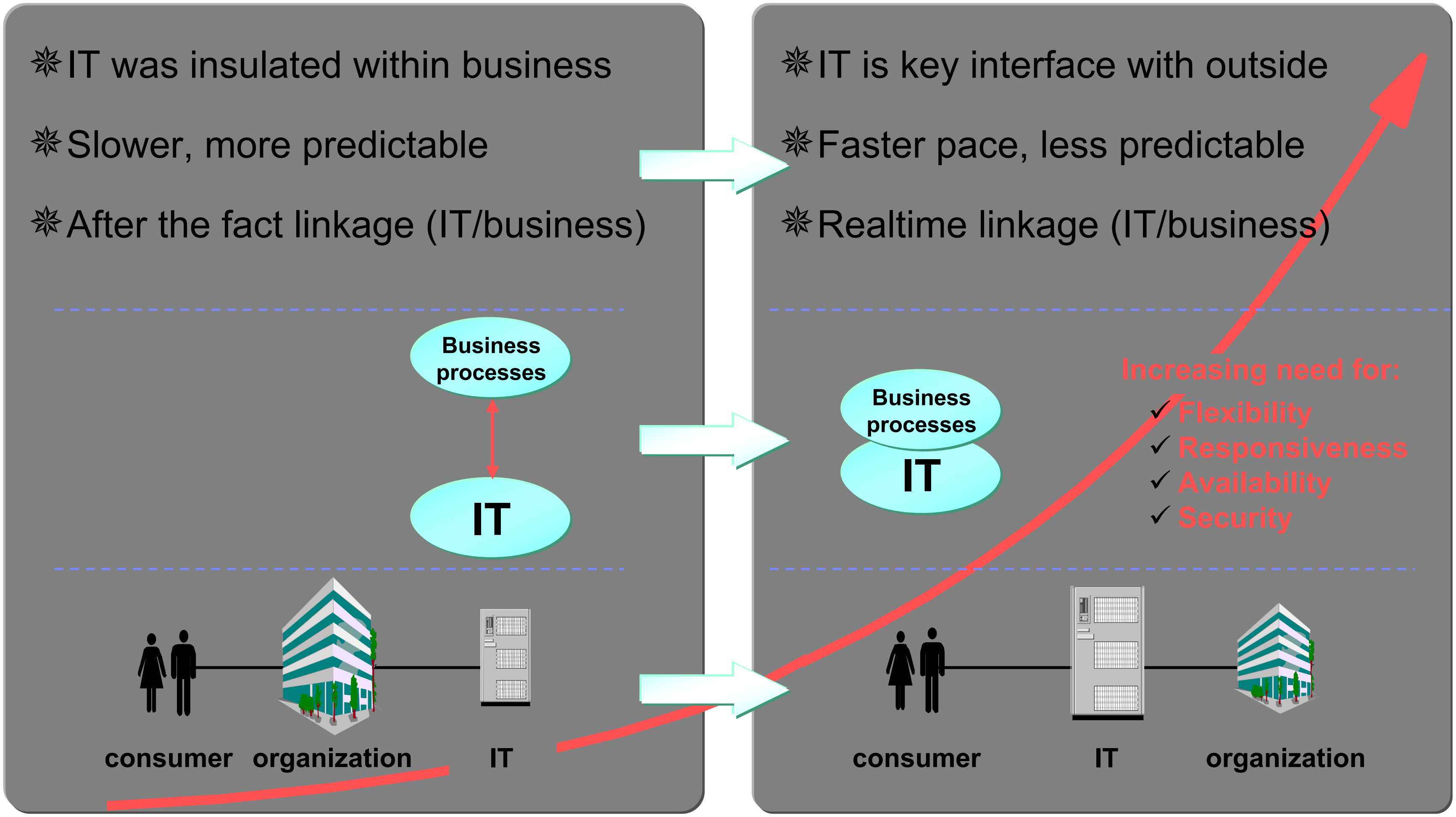
IT Arhitect, CISSP

IBM Slovenija, Globalne storitve

Vsebina

- Informacijska varnost
- Varnost v Linuxu – od tračev do znanosti
- Obvladovanje varnosti (Linux sistemov)

Spremenjeni položaj IT v poslovnem procesu



- IT was insulated within business
- Slower, more predictable
- After the fact linkage (IT/business)

- IT is key interface with outside
- Faster pace, less predictable
- Realtime linkage (IT/business)

Increasing need for:

- ✓ Flexibility
- ✓ Responsiveness
- ✓ Availability
- ✓ Security

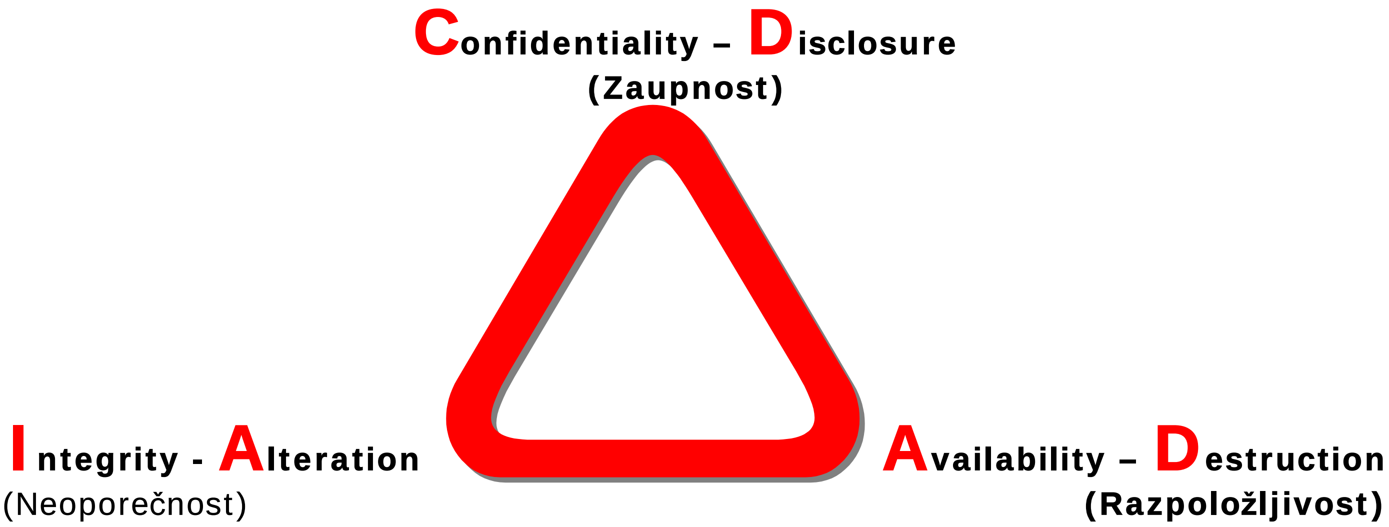
Kaj je informacijska varnost

...is the **protection of information systems** against

1. unauthorized access to or modification of information, whether in storage, processing or transit, and
2. against the denial of service to authorized users or
3. the provision of service to unauthorized users,

Including those measures necessary to detect, document, and counter such threats.

(U.S. National Information Systems Security Glossary)



Confidentiality – Disclosure
(Zaupnost)

Integrity - Alteration
(Neoporečnost)

Availability – Destruction
(Razpoložljivost)

6 najbolj neumnih idej v Informacijske varnosti

(MJR: The Six Dumbest Ideas in Computer Security: http://www.ranum.com/security/computer_security/editorials/dumb/)

1. Default Permit
   Varnost se začne na točki “Deny all”
2. Enumerating Badness
   Kaj je lažje: našteti kaj se sme ali kaj se ne sme izvajati?
3. Penetrate and Patch
   Pri slabem designu produkta nobeno krpanje ne pomaga
4. Hacking is Cool
   Hacking je socialni, ne tehnični problem
5. Educating Users
   Do sedaj še ni uspelo izobraziti uporabnike, da ne bi masovno odpirali neznano pošto
6. Action is Better Than Inaction
   Pogosto je lažje nenarediti neumnost, kot narediti nekaj pametnega.

Miti o Linux (ne)varnosti

1. All distributions are equally secure, or insecure, right out of the box.
   Linux Security *by default* is better or worse than Windows.
   Open source automatically, absolutely equals security--or insecurity.
   My distribution is more secure than your distribution.
   Windows NT is more secure than Linux because it has a C2 rating.
   My operating system is more secure than Linux.
2. Linux is insecure because it is a free operating system.
   Linux is insecure because there is no toll-free support number.
3. A Linux system can be infected by a virus.
   Linux can be infected by DOS viruses if you run Samba.
4. Windows only gets attacked most because it's such a big target, and if Linux use (or indeed OS X use) grew then so would the number of attacks.
5. Open Source Software is inherently dangerous because its source code is widely available, whereas Windows 'blueprints' are carefully guarded by Microsoft.
6. Statistics 'prove' that Windows has fewer, less serious security issues than Linux, that Windows issues are always fixed, and that they are fixed faster.
7. Sendmail is a big security risk - you should be using FooBarMail.

SANS: seznam ranljivosti in priporočila

Top Vulnerabilities to UNIX Systems

1. BIND Domain Name System
2. Web Server
3. Authentication
4. Version Control Systems
5. Mail Transport Service
6. Simple Network Management Protocol (SNMP)
7. Open Secure Sockets Layer (SSL)
8. Misconfiguration of Enterprise Services NIS/NFS
9. Databases
10. Kernel

Top Vulnerabilities to Windows Systems

1. Web Servers & Services
2. Workstation Service
3. Windows Remote Access Services
4. Microsoft SQL Server (MSSQL)
5. Windows Authentication
6. Web Browsers
7. File-Sharing Applications
8. LSAS Exposures
9. Mail Client
10. Instant Messaging

Linux CC certifikacije

CAPP – controlled access protection profile

EAL3 – methodicaly tested and checked

EAL4 – methodicaly designed, tested and reviewed

EAL5 – semiformally designed and tested

ALC_FLR.2 – Life cycle support / Flaw reporting procedures

ALC_FLR.3 – Life cycle support / Systematic flaw remediation

Jan. 2004	SuSE Linux Enterprise server v8 SP3, RC4 w/ certifcation-sles-eal3 package: **CAPP/EAL3+ ALC_FLR.2**
Avg. 2004	Red Hat Enterprise Linux 3, Update 2: **CAPP/EAL3+ ALC_FLR.3** za verzijo WS na xSeries in za verzijo AS na xSeries, iSeries, pSeries, zSeries in Opteron
Sep. 2004 →	Mandrake: **EAL5**. Triletni projekt
Mar. 2005	SuSE Linux Enterprise server v9 w/ certifcation-sles-eal4 package: **CAPP/EAL4+**
še traja	Red Hat Enterprise Linux 4, Update 2: **CAPP/EAL4+ ALC_FLR.3**

Linux varnostna orodja

Ojačani kernel: SELinux, Bastille, grsecurity

Pregled varnosti: Nessus, NSAT, Nmap, SATAN, Saint, Messala, Kismet,
strežniški: COPS, TARA, tiger

Požarna pregrada: ipchains-firewall, Juniper Firewall Toolkit, TIS Internet Firewall Toolkit, netfilter, ipfilter, freestone, gShield, Fire Gnome

IDS, IPS: LIDS, Secure-Linux patch, Dragon IDS, PortSentry, Secure Net Pro, Snort, Shadow, AAFID2

Vabe: Honeyd, Deception Toolkit, FakeBO, Netbusd

Avtentikacija, dostop: Kerberos, GnuPG, tcpwrapper, FreeS/WAN, deslogin, OPIE, S/KEY, Shadow password, HostSentry, NIS, NIS+

Zaupnost: OpenSSH, LSh, OpenSSL, NIST IPSec, TCFS, rsaeuro

Integriteta/neoporečnost: Posix ACL, Trustees, Tripwire, Aide

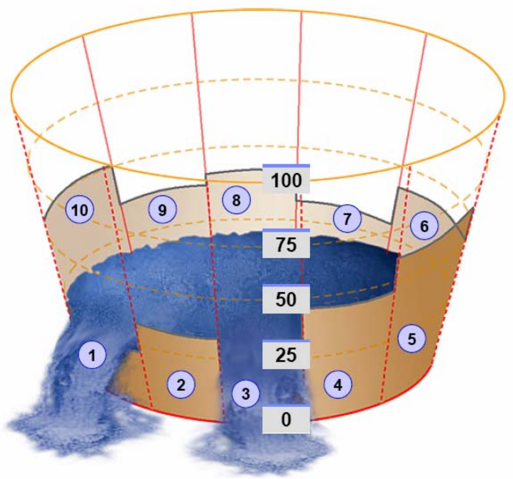
VPN: VPNd, VTun, PPTP-Linux, PoPToP, Tinc

Anti-virus: Symantec, TrendMicro, F-Secure, Kaspersky Lab, Sophos, Grisoft, ClamAv

Torej je Linux varen, ne?

Kaj še manjka:

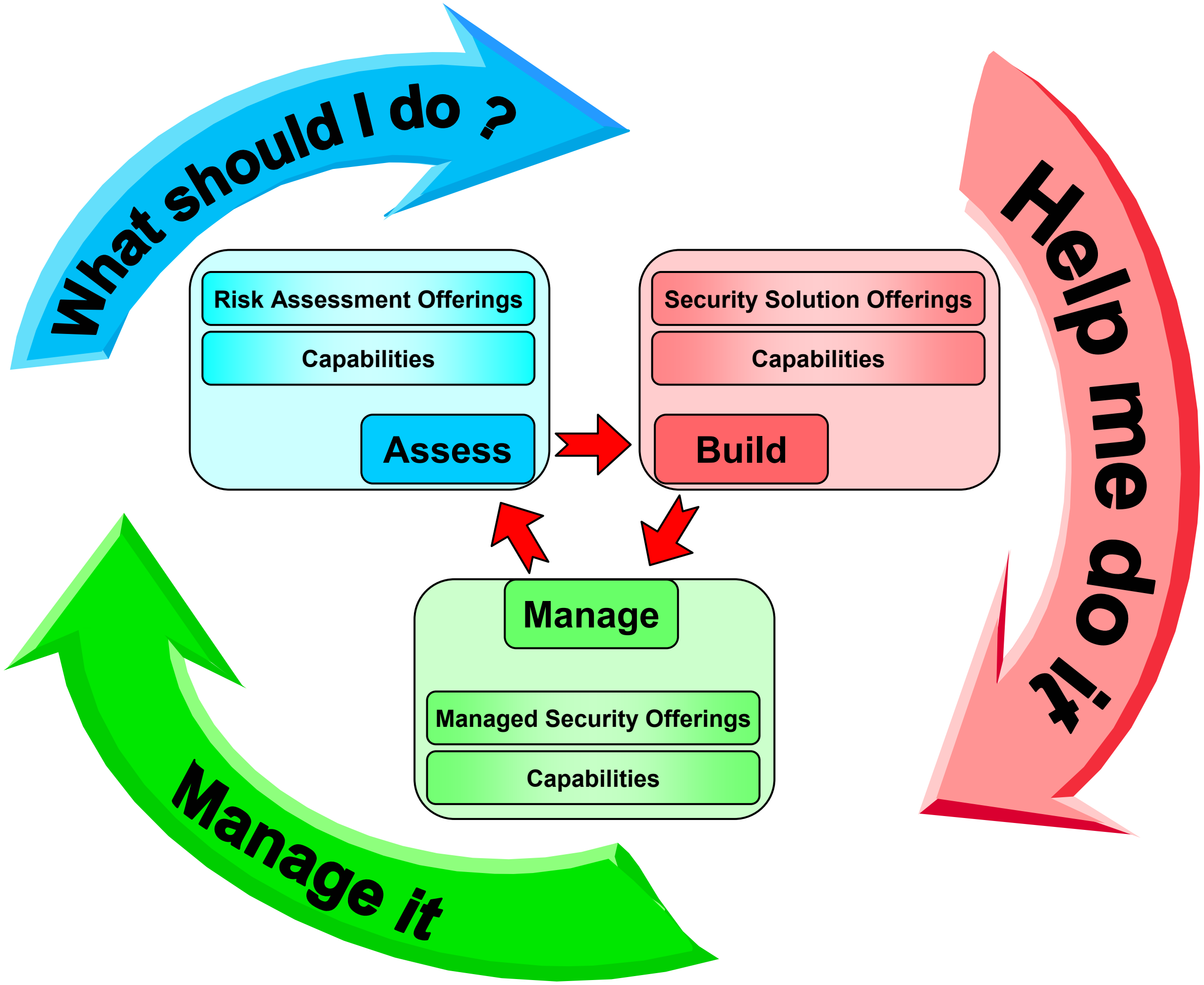
- Ugotoviti, kaj varujemo (kaj in koliko je to pomembno za podjetje)
- Usposobiti administratorje sistemov
- Pridobiti podporo poslovodstva
- Vpeljati varnostno politiko
- Izobraževati uporabnike
- Uskladiti varnostni pristop s poslovnimi partnerji
- Vpeljati procese, ki zagotavljajo delovanje varnostnih
  mehanizmov



1. Security policy
2. Organizational security
3. Asset classification and control
4. Personnel security
5. Physical and environmental security
6. Communications and operations mgmt.
7. Access control
8. Systems development and maintenance
9. Business continuity management
10. Compliance

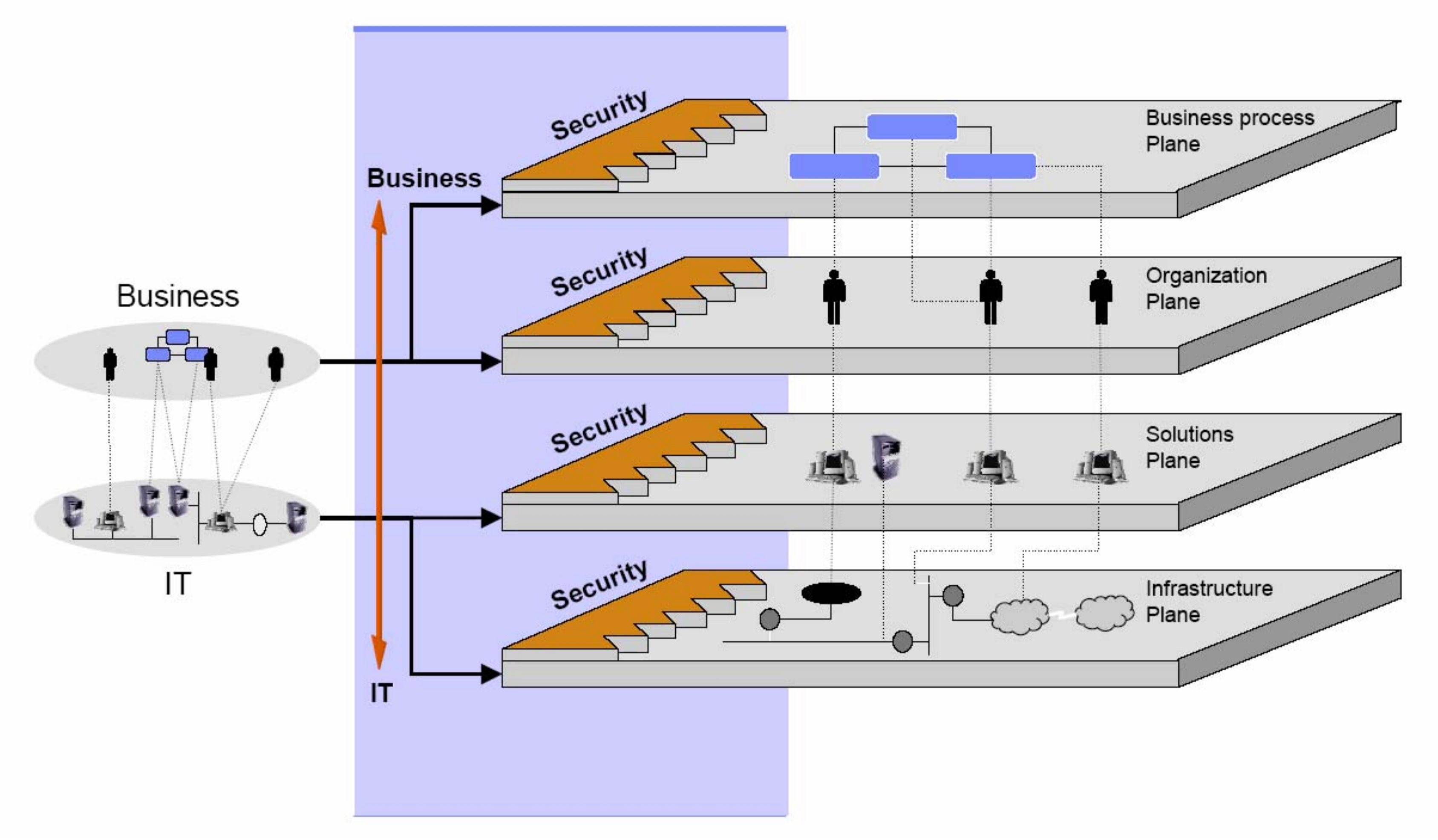
Source: ISO/IEC 17799 – Code of Practice for Information Security Management

Upravljanje informacijske varnosti



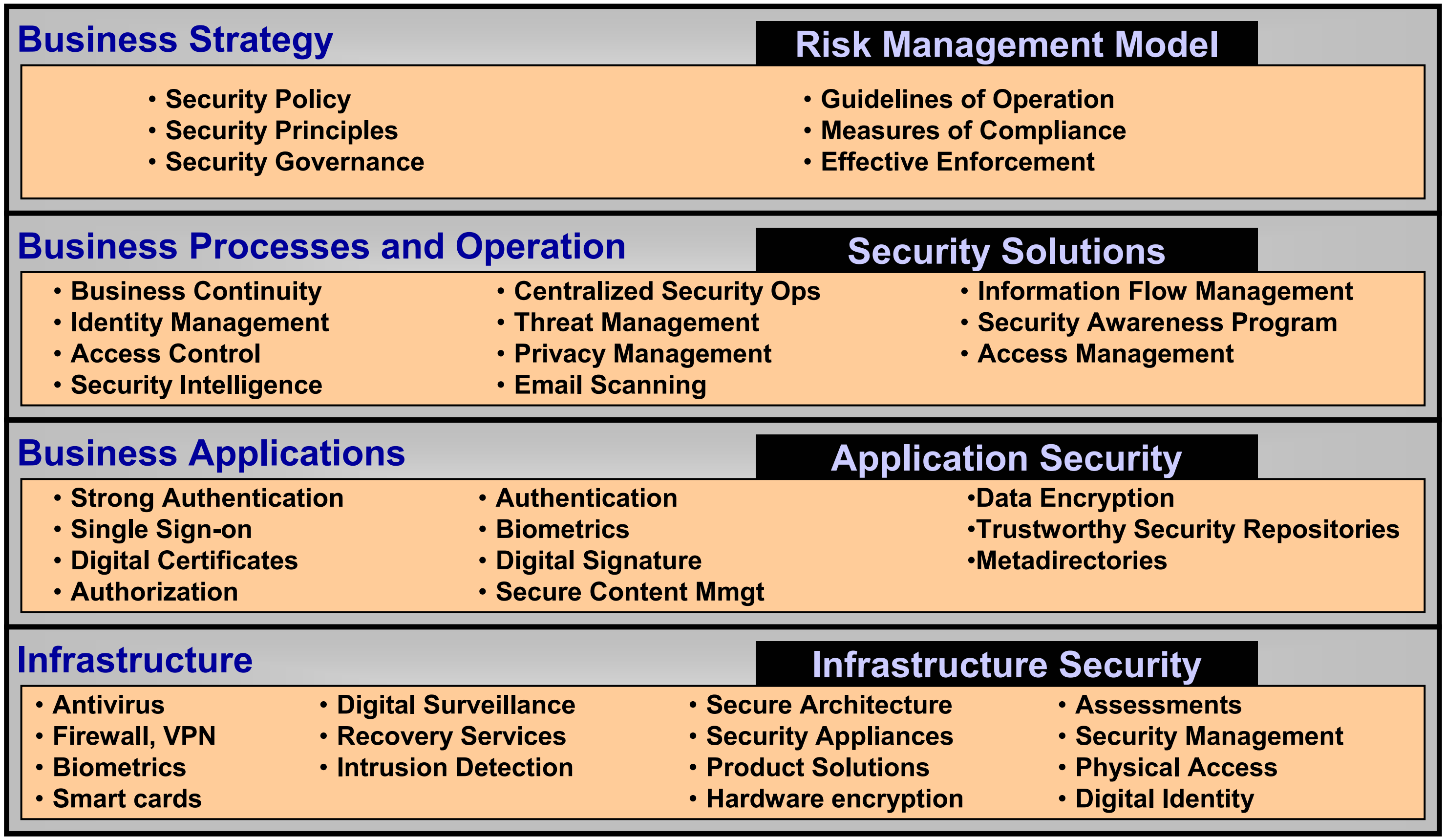
Security Is A Continuous Process, Which Should Be Integrated Into The Enterprise System Management

Nivoji informacijske varnosti



Nivoji informacijske varnosti (II.)

Security must be managed and integrated at the enterprise level.
It is about business, not technology



Business Strategy

Risk Management Model

- Security Policy
- Security Principles
- Security Governance
- Guidelines of Operation
- Measures of Compliance
- Effective Enforcement

Business Processes and Operation

Security Solutions

- Business Continuity
- Identity Management
- Access Control
- Security Intelligence
- Centralized Security Ops
- Threat Management
- Privacy Management
- Email Scanning
- Information Flow Management
- Security Awareness Program
- Access Management

Business Applications

Application Security

- Strong Authentication
- Single Sign-on
- Digital Certificates
- Authorization
- Authentication
- Biometrics
- Digital Signature
- Secure Content Mmgt
- •Data Encryption
- •Trustworthy Security Repositories
- •Metadirectories

Infrastructure

Infrastructure Security

- Antivirus
- Firewall, VPN
- Biometrics
- Smart cards
- Digital Surveillance
- Recovery Services
- Intrusion Detection
- Secure Architecture
- Security Appliances
- Product Solutions
- Hardware encryption
- Assessments
- Security Management
- Physical Access
- Digital Identity

Celovita implementacija varnosti

	Policies	Services	Capabilities
5 Cross-Industry Value Coalition	•Policy Integration •Standards Integration •Trust Chain Compliance	•Trust Chain Assessment •Trust Chain Intelligence •New Transport Design	•Business Risk Mgmt •Autonomic Security •Dynamic Identification
4 Industry-Centric Value Web	•Federated Identification •Scenario-based Policies •Pervasive Commerce Rules	•Marketplace Management •Business Process Definition •p-Commerce Design & Impl	•Web-Based Delegation •Automated Actions •Pervasive Commerce Mgmt
3 Value Chain Visibility	•Role-Based Definitions •Independent Privacy Cert •Trust Profile & Process	•Enterprise Security Program •Privacy Strategy & Impl •Secure Solution Design's)	•Identity Management •Privacy Management •Integrated Management
2 Select 'Trusted' Partners	•Standards Definition •Process Development •Information Asset Profile	•Enterprise Risk Assessment •Ethical Hacking •Internet Security Architecture	•Access Management •Threat Management •Intrusion Detection
1 Isolated Operations	•Health Check •Policy Definition •Physical Security	•Fast Track Assessment •Workshops: Align Bus & IT •Employee Education	•Firewall/Encryption Systems •AntiVirus Solution •Secure Servers and PCs

Obramba informacijskega sistema

Razumevanje varnostnega stanja

- Varnostne politike sprejete in vpeljane
- Varno konfigurirani in preverjani sistemi

Gradnja obrambe

- Prilagoditev varnosti specifičnim zahtevam
- Pristop k varnosti s poslovnega vidika
- Izobraževanje in osveščanje uporabnikov

Odkrivanje varnostnih kršitev

- Odkrivanje napadov, preden postanejo resni
- Stalna opreznost

Odziv na varnostne incidente

- Obvladovati, zatreti, okrevati
- Vedeti kaj in kako narediti, preden se zgodi
- Čas je pomemben
- Poiskati pomoč