IS/IT outsourcing services

RNDr. Stanislav Vojíř, Ph.D.
Michelfeit

CONTENTS

- **Introduction in Security wintin Service Oriented Organization**
- **Internal and Customer Security Standards**
- **Internal Processes within the Service oriented Organization**

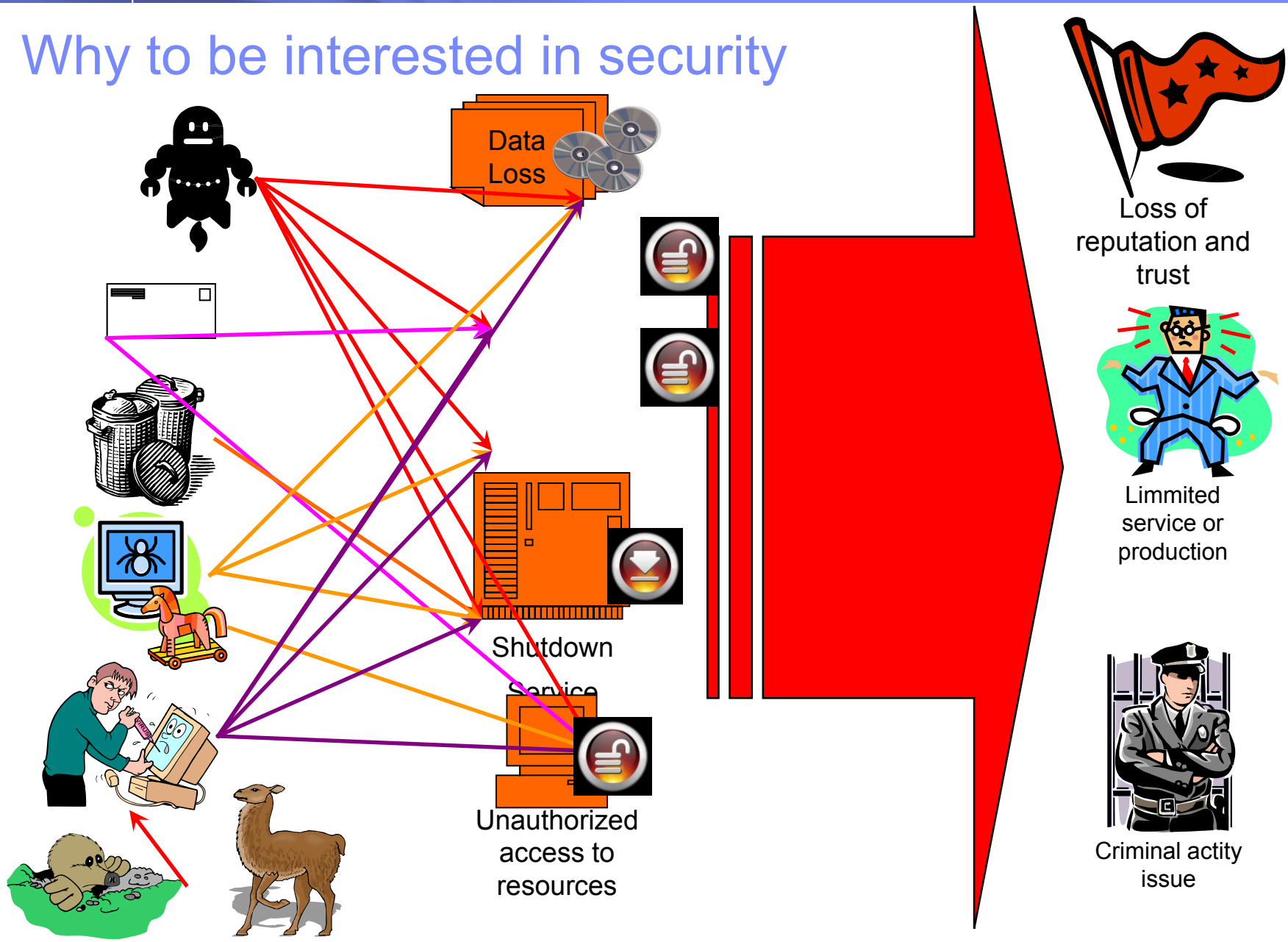
Motivation

- 257a - Poškození a zneužití záznamu na nosiči informací
- Kdo v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch získá přístup k nosiči informací a
  - takových informací neoprávněně užije,
  - informace zničí, poškodí nebo učiní neupotřebitelnými, nebo
  - učiní zásah do technického nebo programového vybavení počítače, bude potrestán **odnětím svobody až na jeden rok** nebo zákazem činnosti nebo peněžitým trestem nebo propadnutím věci.

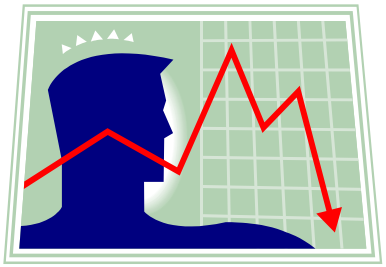
- **Odnětím svobody na šest měsíců až tři léta** bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 jako člen organizované skupiny, nebo způsobí-li takovým činem značnou škodu nebo získá-li sobě nebo jinému značný prospěch.
- **Odnětím svobody na jeden rok až pět let** bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 škodu velkého rozsahu nebo získá-li sobě nebo jinému prospěch velkého rozsahu.

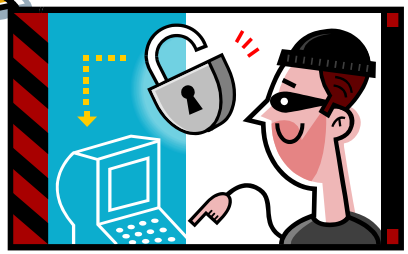
- Czech republic law: 257a - Missuse of connectivity or benefiting from unathorized access to data medium or information
  - **imprisonment for six months to three years**
  - **imprisonment for one to five years - large-scale damage**

Why to be interested in security



Why to be interested in security





Prevention

- **Education of responsible and interested**
- **Set roles and access rights**
- **Appropriate software**
- **Regular software updates**
- **Following basic rules**
- **Regular inspection**
- **Active inspection**
- **Physical security**
- **D / R procedure**

Education of responsible and interested

- **Education of responsible persons**
- **User Traning**
- **Information for Customer**
- **Maintaining a high level of knowledge**
- **Current status**
- **Warning against current threats**

Set roles and access rights

- **Set roles and access rights based on business need**
- **User roles and groups to lower the security maintenance cost**
- **Remember non- PC devices**
  - Network
  - Mobile devices
  - Printers
  - Restricted areas
- **Follow internal processes**

Appropriate software

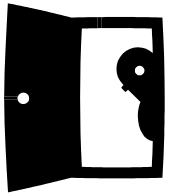
- **Appropriate OS**
- **Security policy SW**
- **Firewalls**
- **Antivirus SW**
- **Further SW based on need (anti-spam, anti-spyware, monitors, etc.)**
- **SW needed for production which support security**

Regular software updates

- **Regular OS update**
- **Regular SW update**
- **Regular Antivirus DB update**
- **Regular maintenance of DB with user roles and access rights**

Following basic rules

- **Any security rules are useless if the people inside the company behave irresponsibly**
- **Good password**
- **Personal responsibility**
- **Social engineering**



Regular inspection

- **It is necessary to regularly check**
  - System
  - users and roles DB
    Setting of key applications
- **Found deviations must be quickly removed**
- **All checks must be properly documented**

Active inspection

- **Monitoring of network traffic**
- **Monitoring of System operation**
- **Ethical hacking**

Physical security

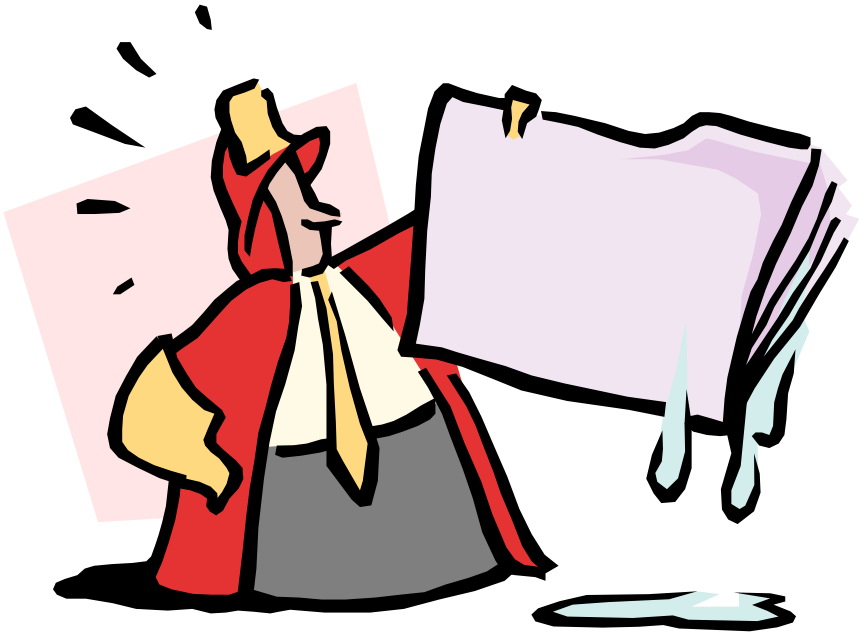
- **Possible threats**
  - Unauthorized access
  - Damage
  - Theft
  - Unintentional injury
  - Damage by fire or natural disaster

Physical security

- **Placing HW into rooms with a dedicated access**
- **Fire Security**
- **Backup power**
- **Backups location in another place**
- **Minimize the movement of foreign persons in buildings**
- **Use of electronic security, cameras, security agencies**

D / R procedure

- **Regular Backups**
- **Secure Data Storage**
- **Plan in the event of failure or damage**



Internal and customer security standards and policies

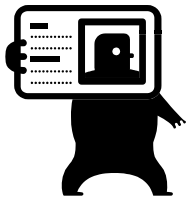
- **Examples of standards and policies:**
  - Internal (company)
    - ITCS300 - Basic IT staff rules
    - ITCS104 - IT Security Rules
    - CIO104 - IT Security
    - LEG116 - Classification and management of Materials
  - Public
    - ISO / IEC DTR 13335-1 Information technology
    - ITIL - Security Management

Internal and customer security standards and policies

- **Identification**
- **Authentication**
- **Authorization**
- **Privacy and confidentiality of information**
- **Reliability and availability of services**
- **Audit**
- **Review**
- **Reporting and management of security incidents**
- **Managing physical access**

Internal and customer security standards and policies

- **Identification**
  - Unique key for each user
  - Digital Certificates created and validated by CA



- **Group 1: Key applications and data storages needed for core bussiness**
- **Group 2: SWs or data storages with clasified informations, parts of key processes or subject of certification (audit)**
- **Group 3: Other BAU SW**
- **Group 4: Traninf, test and development systems.**

Internal and customer security standards and policies

- **Authentication**
  - User-authentication system
    - Verification of user identity
    - Passwords must meet prescribed rules
    - Times applicable passwords must be protected
    - Authentication tokens must be protected
  - System-system authentication
    - Can be used noon expiration password

Internal and customer security standards and policies

- **Authorization**
  - Access must be authorized by owner of the application with regard to the actual needs of access, but access to the application having access to restricted information must be separately approved.
  - Access by a third party to internal services must be authorized by the corporate management, in parallel with providing only the strictly necessary access rights.
- **Remote access for employees**
  - Remote access to corporate networks must be carried out only in an approved manner.
- **Warning**
  - When you log into the internal company network must be displayed warning and guidance.
- **User Resources**
  - Service provider must set the initial provision of the means provided by users.
  - Application and data storage that allows users to manage access rights to their own resources, must contain a tool to perform this management.

Internal and customer security standards and policies

- **Protection and confidentiality of information**
  - Is a set of technical and procedural measures designed for the purpose of preventing unauthorized access to protected corporate data, personal information of employees, business partners, customers and site visitors.
  - Media containing sensitive data must be properly labeled.
- **Residual information**
  - It is necessary to ensure illegibility residual classified or personal data in ways suitable for the medium.
- **Encryption**
  - Company information relevant to an unpublished technology, business plans, financial information and nonpublic personal information such as credit card numbers, financial or medical records must be encrypted when sent through the Internet.

Internal and customer security standards and policies

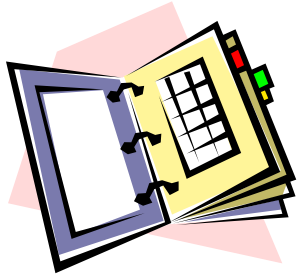
- **Reliability and availability of services**
- **Managing system resources**
  - System resources must be protected from normal users
  - Regular user permissions must be based on the business needs, determined by service provider or owner of the application.
- **Malware**
  - It is necessary to have an active technical tools to prevent the spread and run malicious code.
  - Application developers must provide written assurance that the antivirus test conducted as part of the final tests.
- **Monitoring weaknesses**
  - According to the type of network you have to choose tools, timing and extent of monitoring weaknesses.
- **Warning system - security patches**
  - Is necessary to set the process for timely installation of patches.
  - It is must to upgrade OS to a supported OS with respect to the end of support for the OS. This upgrade may be delayed for extended support for security patches.
- **Modification Center**
  - Any modification of application software must be approved by corporate management and the installation of such software must go through the approval process.
- **Availability of**
  - It is necessary to have an active technical tools to prevent the DoS attack
  - It is necessary to have an active technical tools to prevent and detect unlimited number of unsuccessful attempts to log on to the service.
  - It is necessary to have a process for detecting and processing of systematic attack.

Internal and customer security standards and policies

- **Setup Audit**
- **For systems, applications, data storage, network equipment, where it is technically possible it is necessary to log an alert :**
  - successful and unsuccessful login attempt
  - Modification of system resources
  - Attempt to read system resources, which will be labeled as an exception.
  - Attempt to run system resources that will be labeled as an exception. All activities conducted with Security Administrator authority. Successful assignment and allocation of IP addresses.
- **For internal services should be alert for:**
  - All attempts to remote access to internal company network.
- **Internal log cannot be stored on customer environment.**
- **Audit records must include the date, time, type a user identification**
- **Audit records must be stored for 60 days.**

Internal and customer security standards and policies

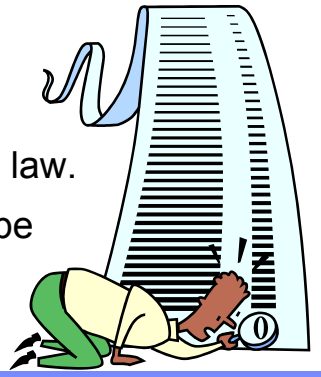
- **Health check**
  - It is necessary to carry out a health check at regular intervals.
- **Verification of the security procedures**
  - Security procedures must be regularly checked on representative samples
- **In-house acreditations and certification**
  - The method and implementation of tests and checks must be changed whenever a service is changed.
  - It is necessary to carry out an annual recertification for all intra-company services.



Internal and customer security standards and policies

- **Reporting and management of security incidents**
- **It is necessary to contact the responsible person and inform them of:**
  - Contact persons for the management and technical area.
  - Description of the problem, the extent of systems or data that have been affected by the incident, already performend activities.
- **Immediately create a record containing all information regarding the incident. For each piece of information is necessary to state the date and time.**
- **Technical support must begin actions to mitigate the consequences, without delay.**
- **Responsible persons will provide information and instructions on how to proceed.**

- **It Is wrong:**
  - Conduct investigations on your own. Risk may be premature disclosure of an investigation or modifying records.
  - Contact the persons or companies suspected of causing the incident, without direct instruction responsible person.
  - Try to go attack the attacker (the System). Such behavior is easily reaches beyond the law.
  - Try to clean up (delete data), without direct instruction responsible person. Risk could be loss of data necessary to discover the cause.



Internal and customer security standards and policies

- **Managing physical access**
- **Physical protection of systems and networks**
  - System and network equipment must be protected against damage and theft.
  - Each entry into the protected area must be secured.
- **Physical protection and inventory of media**
  - Media containing key data, backups, archive data and D / R must be physically protected from unauthorized access, theft and damage.
  - Protected library media must be inspected at least once a year.

Internal and customer security standards and policies

- **Operating Systems**
  - AIX Platforms
  - Linux Servers
  - Microsoft Windows 2008 Servers
  - Microsoft Windows 2003 Servers
  - Microsoft Windows 2000 Servers
  - Microsoft Windows NT Servers
  - Novell Netware
  - OS/2 based OS
  - OS/400 Platforms
  - zOS, OS390 and MVS Platforms
  - z/VM and VM Platforms
  - VMWare ESX/GSX Servers

- **Application software / middleware**
  - Apache Web Servers
  - DB2 Universal Databases
  - Lotus Domino Servers
  - Netview
  - OS/2 LAN Servers
  - Websphere Application Server
  - SSH Servers
  - Samba

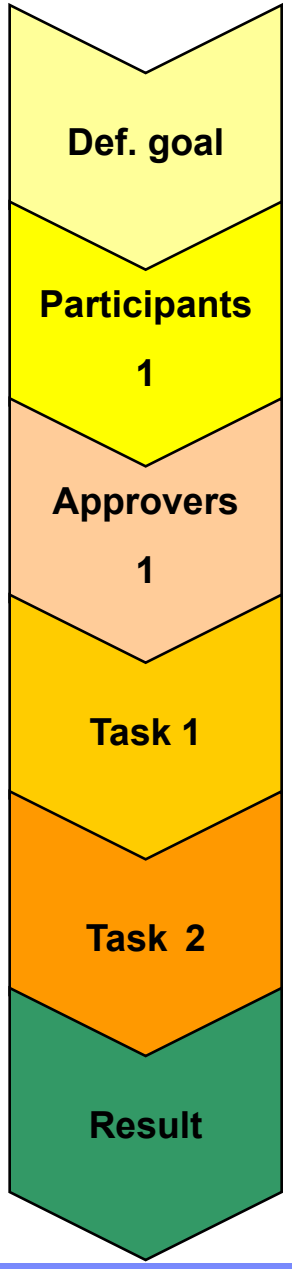
- **Network infrastructure**
  - Local Area Network (LAN) equipment
  - Wireless Equipment
  - Firewalls

- **Voice infrastructure**
  - Avaya Media Server
  - Cisco Call Manager
  - Call Management System

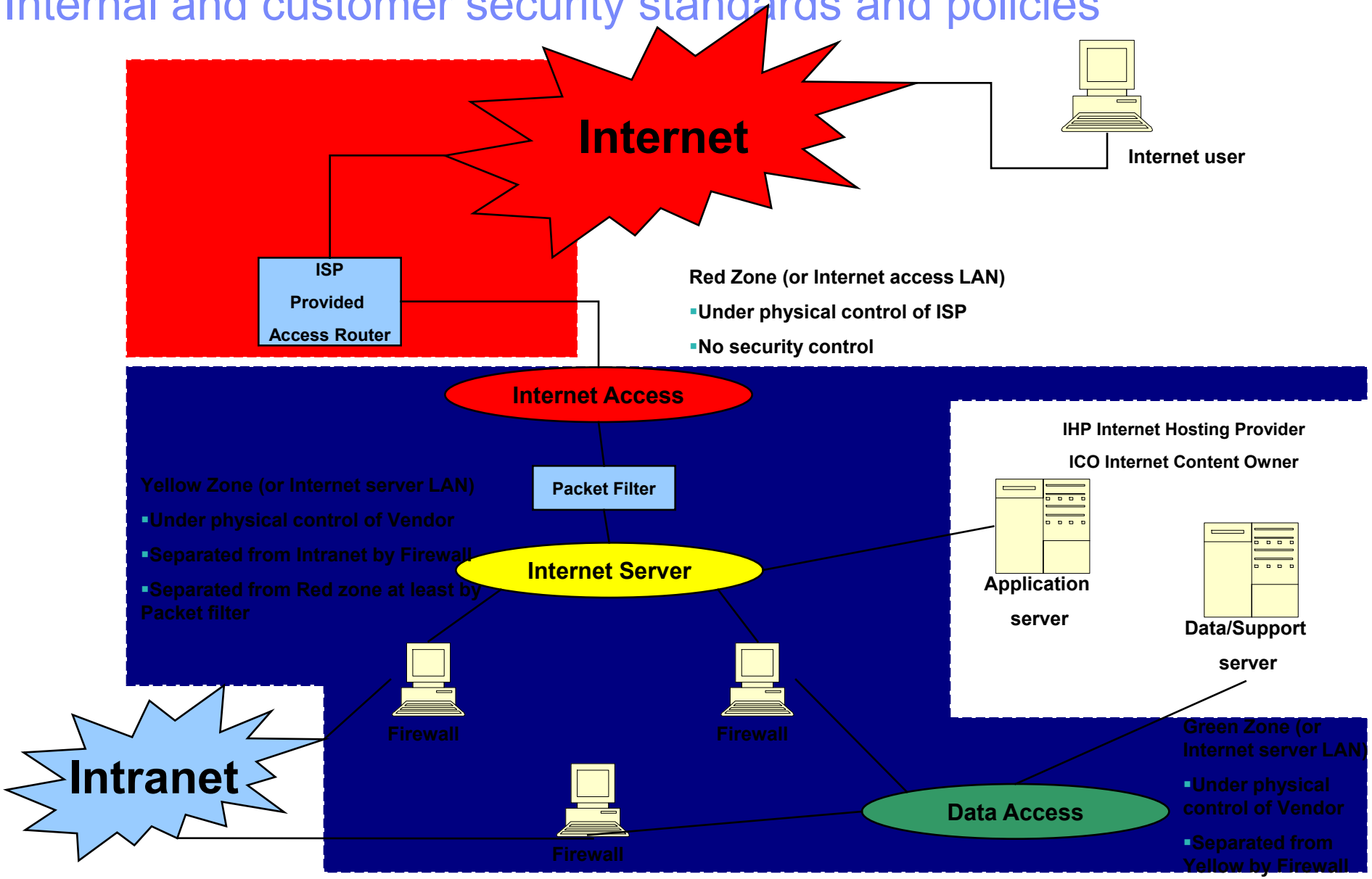
- **Other devices**
  - Printers
  - Industrial devices
  - Remote terminals

Internal and customer security standards and policies

- **The process is**
  - Long time
  - event driven
  - structured sequence of activities that require a
    - People
    - Information
    - Technology
- **in order to achieve the objective.**

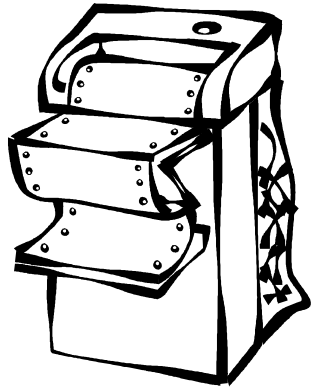


Internal and customer security standards and policies



Internal and customer security standards and policies

- **Physical security controls**
  - Areas
  - Devices
  - Prints
  - Responsibility only for own premises, not the customer's premises



Internal and customer security standards and policies

- **Encryption**
  - Secure method
  - Performance and recovery issues
  - Law restrictions

Questions?