Information Security
Protecting the Global Enterprise
Donald L. Pipkin, Hewlett-Packard Company
Prentice Hall PTR
Upper Saddle River, New Jersey 07458
www.phptr.com

1. Information Security – Bezpieczeństwo informacji

1.1 Information is a Business Asset – Informacja ma wartość biznesową
Confidentiality
Accuracy
Availability

1.2 Security is a business Process - Bezpieczeństwo jest procesem biznesowym – kopromis między kontrolą a łatwością użycia. Miary bezpieczeństwa zależne od wartości informacji:
Access - Dostęp
Identification - Identyfikacja
Authentication - Uwierzytelnienie
Authorization - Autoryzacja

1.3 Information Security is a Business Requirement – Bezpieczeństwo informacji jest wymaganiem biznesowym. Dodatkowe miary (kryteria bezpieczeństwa):
Accountability – Rozliczalność
Awareness – Świadomość
Administration – Administrowanie

2. Tworzenie planu bezpieczeństwa informacji – fazy
The five main phases of an information security plan are as follows;

2.1 **Inspection** - The most important tasks in developing an Information Security Plan are identifying the key corporate functions, the capabilities they need, when they need those capabilities, and how they interact with other functions. The inspection phase evaluates the security needs of the organization, as well as its current level of preparation.

2.2 **Protection** - Proactive risk reduction includes any process that is in place to prevent a business interruption, such as identifying and qualifying second sources, purchasing spare equipment, expanding product pipeline duration, backing up critical documentation, and outsourcing operations if necessary. In this phase, decisions are made as to what needs protection, what level of protection is required, and how to best implement this level of protection. This is accomplished by creating a comprehensive security design.

2.3 **Detection** - Reactive risk reduction includes any process that is in place to minimize the losses from an incident that could cause an interruption of business processes. This phase explores the process of detecting misuses by examining the attacker, the methods of attack, and the technologies that are used to detect them.

2.4 **Reaction** - The emergency response plan determines how to respond when there is a security incident. It must define the process of responding to probable scenarios. The response must be identified, documented, and tested before there is an incident so that everyone knows what to do during the crisis. The incident response plan is a critical part of the business continuity plan. Preparation is key to a successful response.

2,5 **Reflection** - When the security incident is over and the smoke clears, the organization must perform follow-up steps to be able to put the incident behind and move forward.. The processes that need improvement will undoubtedly be processes that are defined in the business continuity plan. As these improvement are evaluated, a big picture view is needed to see if there are other areas of the business continuity plan to which these changes would be beneficial, or if the changes would impact other areas of the plan.

Every organization needs to review its information security plans. During this process many will discover their business plans do not address the issue of information security. Global security direction must be created for the organization so that specific policies can be built in a consistent manner.

This book will guide you through the five phases of a security plan, highlighting the key points, emphasizing those areas that are critical to an organization's success, and relating stories to illustrate the possible consequences.

2. Faza I: Inspection
Przegląd – analiza ryzyka

3.1. Defining Resources – Definiowanie zasobów
- People
- Property
- Information
- Infrastructure
- Reputation

3.2. Assessing Threats – Określanie zagrożeń
- Human Errors
- System Failures
- Natural Disasters
- Malicious Acts

3.3. Evaluating Potential Losses – Szacowanie potencjalnych strat
- Denial of service
- Disclosure
- Destruction or Corruption

3.4. Identifying Vulnerabilities – Identyfikowanie podatności
- Security Design Flaw
- Incorrect Implementation
- Innovative Misuses
- Social Engineering

3.5. Assigning Safeguards – Wybór zabezpieczeń

3.6. Evaluate Current Status – Ocena aktualnego stanu – przegląd dokumentacji i testowanie zabezpieczeń.

3.1.1 Identifying Resources
- Information
- Algorithms
- Software
- Equipment

3.1.2 Assigning Ownership
- Creator
- Maintainer
- User

3.1.3 Determining Value
- Cost of Re-creation
- Cost of Unavailability
- Cost of Disclosure

3.1.4 Security Classification

The following factors should be considered when assigning a resource's security classifications:
- * Sensitivity of the information
- * Consequences of disclosure
- * Legal and contractual obligations and penalties
- * Standards and Guidelines
- * Information lifecycle

Confidentiality
Availability
Integrity

Checklist

3.2 Threat Assessment

The goal of a threat assessment is to understand the type of threat and the likelihood that the threat will cause a loss.

* Threat identification
* Likelihood assessment

3.2.1 Human Error
3.2.2 Natural Disasters
3.2.3 System Failure
3.2.3.1 Hardware
3.2.3.2 Software

* Software complexity
* Software evolution
* Software testing
* Change management

3.2.3.3 Infrastructure
3.2.3.4 Malicious Acts

* Evaluate Yourself as a Target

3.2.3.5 Malicious Software

* Buffer Overflow
* Logic Bomb
* Parasite
* Sniffer
* Spoof
* Trojan Horse
* Virus
* Worm

3.2.3.6 Collateral Damage

* The Proximity Problem
* Guilt by Association

Checklist

3.3 Loss Analysis

Denial of Services
Theft of Resources
Deletion of Information
Theft of Information
Disclosure of Information
Corruption of Information
Theft of Software
Theft of Hardware
Disruption of Computer Controlled Systems

Checklist

3.4 Identifying Vulnerabilities
3.4.1 Location of Vulnerabilities

Hardware
Software
Infrastructure
Processes

3.4.2 Known Vulnerabilities
3.4.3Security Design Flaw
    Outlived Design
    Software Sources
    Software Development
    Software Security Testing
        * Buffer overflows
        * Race conditions
        * Exception handling
        * Software interfaces
3.4.4 Innovative Misuses
3.4.5 Incorrect Implementation
    Initially Unsecured
    Enable Security Features
    Administration
    Documentation
3.4.6 Social Engineering

Checklist

3.5. Assigning Safeguards
In all cases, safeguards must be consistent, comprehensive and cost effective.
3.5.1 Avoidance
    Reducing Threats
    Removing Vulnerabilities
    Limit access
    Adding Safeguards
3.5.2 Transference
    Insurance
    Outsourcing
3.5.3 Mitigation
    Reduce Scope
    Improved Detection
    Rapid Response
3.5.4 Acceptance

Checklist

3.6. Evaluation of Current Status
3.6.1 Assessment
3.6.2 Comprehensiveness
    Industry Standards
    Quality
    Conformity
3.6.3 Testing
    Static Analysis
    Dynamic Analysis
        * Electronic Security
        * Physical Security
        * Biological Security
3.6.4 Business Impact Analysis

Checklist

Faza II: Protection
Ochrona – uwzględnienie kryteriów bezpieczeństwa na każdym poziomie

Philosophies
Security Vision
    Trust
    Protection
Principles
    Security Architecture
Policies
    Security Strategy
        * Rules
        * Guidelines
Procedures
    Security Framework
Practices
    Security Implementation
        * Responsibilities
        * Schedules
4.1. Awareness - Uświadomienie
4.1.1 Appropriate Use
    Relevance
    Roles
        * Information owners
        * Information custodians
        * Information users
    Responsibilities
    Repercussions
4.1.2 Awareness Program
    Continues
    Comprehensive
    Coherent
    Cost Effective
4.1.3 Design Choices
    Delivery Method
    Message Content
    Timeliness
4.1.4 Implementation Options
    Broad-based Awareness
    Focused Awareness
    Awards and Rewards
    Individual Awareness
4.1.5 Lack of Awareness

Checklist

4.2. Access - Dostęp
4.2.1 Global Access
    Anyone
    Anywhere
    Anytime
4.2.2. Access Methods
The changes in access methods define the major phases in the evolution of computing, listed below.
        * Batch mode
        * Timesharing

* Departmental computing
* Distributed computing
* Global computing
* Pervasive computing

Physical Access
Direct access
Network access
Remote access
Social Access

4.2.3 Access Points as Security Checkpoints

Security Domains
Domains of Trust
Security Perimeter
Connecting Domains of Trust

4.2.4 Access Servers

Network Security

* Switches
* Filters
* Routers
* Firewalls
* Proxies

4.2.5 Host Security

* Connection type
* Connection origin
* Trust

4.2.6 Abuse of Access

Checklist

4.3. Identification - Identyfikacja

4.3.1 Enterprise Identification

Unique
Universal
Verifiable
Unforgeable
Transportable
Easy to Use

4.3.2 Issuance of Identifiers

Private Issuance
Public Issuance

4.3.3 Scope of Use

Small Scope
Large Scope

4.3.4 Administration of Identifiers

Centralized Administration
Distributed Administration

4.3.5 Implementation Options

Naming Standards
Smart Cards

* Physical identification
* Electronic identification

4.3.6 Identity Errors

Checklist

4.4. Authentication - Uwierzytelnienie

4.4.1 Factors of Authentication
- Basic Factors
  - * Something you know
  - * Something you have
  - * Something you are
- Implicit Factors
  - * Physical location
  - * Logical Location
- Multiple Factors

4.4.2 Authentication Models
- Multiple Authentication
- Single Authentication
- Multilevel Authentication

4.4.3 Authentication Options
- Passwords
  - * Reusable Passwords
  - * Onetime Passwords
  - * Challenge-Response Passwords
- Handheld Authentication Devices
  - * Sequence-based
  - * Time-based
  - * Certificate-based
- Biometrics

4.4.4 Authentication Management
- Authentication Server

4.4.5 Subverting Authentication
- Direct Attacks
  - * Guessing
  - * Cracking
- Indirect Attacks
  - * Snooping
  - * Capture and Replay
  - * Session Hijacking
- Social Attacks
  - * Social Engineering
  - * Investigation
  - * Searching
  - * Eavesdropping

Checklist

4.5. Authorization - Autoryzacja
- Authorization and Privilege

4.5.1 What Authorization Provide
- Least Privileges
- Separation of Duties
- Increased Accountability

4.5.2 Granularity of Authorizations
- Course Grain Authorization
  - * Access
  - * Utilization
  - * Modification
  - * Creation
  - * Deletion
  - * Management

Fine Grain Authorization
4.5.3 Requirements
Limited Scope
Globally Defined
Applied to All Entities
4.5.4 Design Choices
Centralized or Distributed
Resource-based or Role-based
List-based or Rule-based
Authorization Server
4.5.5 Abuse of Authorization

Checklist

4.6. Availability - Dostępność
4.6.1 Types of Outages
Unsheduled Downtime
Sheduled Downtime
Peak Usage
4.6.2 Protecting all Levels
Data Availability
System Availability
Application Availability
Infrastructure Availability
* Power Availability
* Network Availability
4.6.3 Availability Models
Resistant
Resilient
Redundant
Replaceable
Restartable
Recoverable
4.6.4 Availability Classifications
4.6.5 Availability Outage

Checklist

4.7. Accuracy - Dokładność
4.7.1 Information Lifecycle
Initially Accurate
Scope of Use
Correlation of Information
4.7.2 Information System Accuracy
Information
* Storage
* Transmition
Transaction
* Reservation
* Communication
* Control
* Rollback
Users
4.7.3 Methods
Limited Use
* Authorizations

        * Applications
    Verification
        * Comparison
        * Calculations
4.7.4 Loss of Accuracy

Checklist

4.8. Confidentiality - Poufność
4.8.1 Information in the Enterprise
    Business Information
    Personal Information
4.8.2 Confidentiality Concerns
    Secure Storage
        * Online
        * Offline
        * Printouts
    Secure Communications
        * Private Network
        * VPN
    Secure Disposal
        * Object Reuse
        * Magnetic Media
        *Physical Forms
4.8.3 Methods of Ensuring Confidentiality
    Compartmentalization
    Encryption
4.8.4 Sensitivity Classifications
    * Company Secret
    * Company Confidential
    * Company Proprietary
    * Internal Use Only
    * Private
    * Public
4.8.5 Invasion of Privacy

Checklist

4.9. Accountability - Rozliczalność
    Accountability and Responsibility
4.9..1 Accountability Models
    Individual Accountability
    Group Accountability
    Chain of Command
4.9.2 Accountability Principles
    Notification
    Identification
    Monitoring
    Auditing
    Alarming
    Enforcement
4.9.3 Accounting Events
    Information Resource Access
    Administrative Actions
    Failure Events
4.9.4 Accountability System Feature

4.9.5 Accountability Failures

Checklist

4.10. Administration - Administrowanie
4.10.1 Enterprise Information Security Administration
Simplification
Automation
4.10.2 Administrative Process
Installation
Configuration
Operations
Maintenance
Monitoring
4.10.3 Areas of Administration
Identification
Authentication
Authorization
Accountability
4.10.4 Administration Errors

Checklist

5. Faza III: Detection
Wykrywanie naruszeń

5.1. Intruder Types – Charakterystyka intruzów
Motives
* Financial
* Social
* Political
* Personal
Relationship
* Insiders
* Outsiders
5.2. Intrusion Methods – Metody naruszeń
Physical Intrusions
Technical Intrusions
Social Intrusions
5.3 Intrusion Process – Przebieg naruszenia
5.4. Intrusion Detection Methods
Profiles
Offline Methods
Online Methods
5.1. Intruder Types – Charakterystyka intruzów
5.1.1 Outside Intruders
Hackers
Competitors
5.1.2 Inside Intruders
Disgruntled Employees
Contract and Temporary Employees
Business Partners
5.1.3 Professional Intruder
Hackers for Hire
Organized Crime
Activists

Terrorists

Checklist

5.2. Intrusion Methods – Metody naruszeń
5.2.1 Technical Intrusions
Hacking
Spying
5.2.2 Physical Security
Business Offices
Home Offices
On the Road
5.2.3 Social Engineering
Selection
* Access
* Willingness
Motivation
* Greed
* Revenge
* Morality
* Group Loyalty
* Recognition
Pretext
* Socializing
* Trusted Advisor

Checklist

5.3. Intrusion Process – Przebieg naruszenia
5.3.1 Reconnaissance - Rekonesans
Public Information
Disclosed Information
* Active Scanning
* Software Fingerprinting
Gathered Information
* Shoulder Surfing
* Dumpster Diving
* Eavesdropping on Communications
5.3.2 Gaining Access – Zbieranie informacji
Breaching the Perimeter
Alternate Entry Points
Physical Access
5.3.3 Gaining Authorizations – Uzyskanie autoryzacji
Impersonation
Session Theft
* Unattended sessions
* Automated sessions
* Session hijacking
Subversion
Covert Software
5.3.4 Achieve Goals – Osiągnięcie celu
Become Famous
Become Rich

Checklist

5.4. Detection Methods – Metody wykrywania naruszeń
Intrusion detection methodologies are based on three processes:
* Signature analysis
* Static-state analysis
* Dynamic analysis
5.4.1 Profiles - Profile
Vulnerability Profiles
System Profiles
Network Profiles
User Profiles
Attack Profiles
Self-Monitoring Profiles
5.4.2 Offline Methods
Configuration Analysis
Vulnerability Analysis
5.4.3 Online Methods
* System-based
* Network-based
* Hybrid Systems
Anomaly Detection
Attack Analysis
Misuse Analysis
Honey Pots
5.4.4. Human Methods

Checklist

6. Faza IV: Reaction
Reakcja

Incident Response Philosophies
Watch and Warn – Obserwacja i ostrzeganie
Repair and Report – Reperacja i raport
Pursue and Prosecute – Ściganie i karanie
Incident Response Plan
Documentation
Determination
Notification
Containment
Assessment
Eradication
Recovery
6.1. Response Plan
6.1.1 Response Procedures
6.1.2 Authority to Respond
Financial Limits
Disabling Services
Disconnection from the Network
Communications
6.1.3 Resources
People
Tools
External Support
6.1.4 Legal Review

Checklist

6.2. Incident Determination
6.2.1 Possible Indicators
- Unfamiliar Files
- Unknown Programs or Processes
- Consumption of Resources
- System Crashes

6.2.2 Probable Indicators
- Activities at Unexpected Times
- Presence of New Accounts
- Reported Attacks
- Notification from Intrusion Detection System

6.2.3 Definite Indicators
- Use of Dormant Accounts
- Changes to Logs
- Presence of Hacker Tools
- Notification by Partner
- Notification by Hacker

6.2.4 Predefined Situations
- Loss of Availability
- Loss of Integrity
- Loss of Privacy
- Violation of Policy
- Violations of the Law

Checklist

6.3. Incident Notification
6.3.1 Internal
- Initial Notification
- Response Team
- Incident Manager
- Management

6.3.2 Computer Security Incident Organizations
- Incident Advisory
- Incident Response

6.3.3 Affected Partners
- Contractual
- Upstream
- Downstream

6.3.4 Law Enforcement
6.3.5 News Media

Checklist

6.4. Incident Containment
6.4.1 Stopping the Spread
- Determine Affected Systems
- Deny Access
- Eliminate Rogue Processes

6.4.2 Regain Control
- Lock out the Attacker
    * Change Passwords
    * Disable Services
    * Remove Back Doors
    * Monitor Activities
- Scrub the System

Rebuild the System
* User Original Media
* Apply Security Patches
* Review Local Customizations
* Reload Data

Checklist

6.5. Assessing the Damage
6.5.1 Determining the Scope of Damage
Compromised Data
Compromised Systems
Compromised Services
Compromised Privileges
6.5.2 Determining the Length of the Incident
6.5.3 Determining the Cause
Vulnerability Exploited
Safeguards Bypassed
Detection Avoided
6.5.4 Determining the Responsible Party
Source of Attack
Online Identity
Attack Fingerprints

Checklist

6.6. Incident Recovery – Odtwarzanie stanu sprzed naruszenia
6.6.1 Setting Priorities
6.6.2 Repair the Vulnerability Usuwanie podatności
Apply a Patch
Disable the Service
Change the Procedure
Redesign
6.6.3 Improve the Safeguard – Udoskonalanie zabezpieczeń
Review Safeguard
Add Safeguard
6.6.4 Update Detection – Modyfikacja metod wykrywania
Configuration Changes
Add Detection
6.6.5 Restoration of Data – Odtworzenie danych
Availability
Integrity
Confidentiality
6.6.6 Restoration of Services – Przywrócenie usług
Availability
Integrity
Confidentiality
6.6.7 Monitor for Additional Signs of Attack – Monitorowanie dodatkowych sygnałów ataku
6.6.8 Restoration of Confidence – Przywrócenie zaufania
Management
Stockholders
Users
Partners
Public

Checklist

6.7. Automated Response – Automatyczna odpowiedź
    Automated Defenses
    Gathering Counterintelligence
    Counterstrike

Checklist

7. Faza V: Reflection
Wyciągnięcie wniosków

Postmortem Documentation
Process Management
    Risk Analysis
    Business Impact
    Emergency Response
    Incident Management Program
    Business Recovery Program
External Follow-up
    Required Financial Reporting
    News Media
    Law Enforcement
7.1. Incident Documentation – Dokumentacja naruszenia
7.1.1 Incident Source Information – Źródła informacji o naruszeniu
    Incident Logbooks
    Help Desk Logs
    Network Logs
    System Logs
    Administration Logs
    Physical Access Logs
    Accounting Logs
    Audit Logs
    Security Logs
    Backups
7.1.2 Incident Timeline – Określenie ram czasowych naruszenia
    Format
        * Graphical Timeline
        * Footnote References
    Content
        * Discovery
        * Determination
        * Investigation
        * Recovery
        * Attacker's Activities
7.1.3 Technical Summary – Podsumowanie techniczne
    Cause
        * Who
        * What
        * How
        * When
        * Where
    Impact
        * Systems
        * Data
        * Down time
        * Recovery

        * People
    Resolution
        * Diagnosis
        * Containment
        * Restoration
    Improvement
        * Remove Vulnerabilities
        * Increase Safeguards
        * Improve Detection
        * Automate Response

7.1.4 Executive Summary – Raport dla kierownictwa

    Cause
        * Why
        * Who
        * When
        * Where
        * How
        * What
    Impact
        * Actual Losses
        * Direct Losses
        * Lost Revenue
        * Lost Productivity
        * Recovery Costs
        * Intangible Costs
    Resolution
    Improvement

Checklist

7.2. Incident Evaluation – Oszacowanie skutków naruszenia

7.2.1 Identity Processes for Improvement

    Process
    People
    Communications
    Tools

7.2.2 Process Improvement

7.2.2.1 Determine Resources Required

    * Equipment
    * People
    * Expertise
    * Time

7.2.2.2 Prioritize

    * Return on Investment
    * Most Visibility
    * Management's Biggest Concerns
    * Quickest to Implement
    * Least Expensive

7.2.2.3 Develop a Project Plan

7.2.2.4 Gain Management Commitment

7.2.2.5 Allocate Resources

7.2.2.6 Implement Changes

Checklist

7.3. Public Relations – Opinia publiczna

7.3.1 The Right People
7.3.2 The right Time
7.3.3 The Right Message
7.3.4 The Right Forum
- Press Release
- Press Conference
- Interview

7.3.5 The Right Attitude

Checklist

7.4. Legal Prosecution – Odpowiedzialność karna
7.4.1 Computer Crime Laws – Prawo o przestępstwach komputerowych
- Writing the Laws
- Interpreting the Laws
- Enforcing the Laws

7.4.2 Jurisdiction - Jurysdykcja
- Extradition

7.4.3 Collection of Evidence – Gromadzenie dowodów
- Documentation
- Chain of Custody
- Data Reduction
- Impact on Operations

7.4.4 Successful Prosecution – Efektywność postępowania karnego
- Sympathetic
- Age
- Appropriate Punishment

Checklist

Epilogue: The Future of Information Security

A World Without Borders
Service-based Architecture
- Access Server
- Identification Server
- Authentication Server
- Authorization Server
- Application Server
- Information Storage Server
- Accountability Server
- Administration Server

Basic Business Principles
- Check and Balance
- Separation of Duties
- Audit Trail

Pervasive Security