

Adatbiztonság a gazdaságinformatikában

Security Policy

Dr. Bencsáth Boldizsár
adjunktus

BME Híradástechnikai Tanszék
bencsath@crysys.hit.bme.hu



2011. november
19.
Budapest

Hierarchy of basic documents

- Policies
 - Policies define the organization's commitment to protecting organization's commitment to protecting the confidentiality, integrity and availability (CIA) of information.
- Procedures
 - Procedures provide guidance on the implementation of the goals and standards implementation of the goals and standards articulated in the security policy.
- Instructions
 - Instructions provide a step-by-step roadmap for implementing technical controls in support of security policies and procedures.

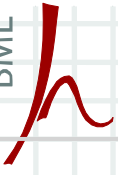
Security policy vs. enforcement

- A security policy is essentially a document stating security goals, and which actions are required, which are permitted
 - Policies may apply to actions by a system, by management, by employees, by system users.
 - A complete security policy is a collection policies (top-level) on specific security issues.
- Do not confuse a policy with an enforcement mechanism
 - Every security policy statement should have a corresponding enforcement mechanism
 - The enforcement mechanism may be a technology (e. g., a firewall), or a process (e. g., security audit)

Security Policies are at Multiple Levels

- High level policies are “human readable”
- High level policies are often at an organizational level and apply to all systems
- High level policies may be refined into multiple low level policies that are apply to system actions, management processes, and actions by employees/users
 - Very general top level policies: “Do not allow malicious code inside our system”
 - For example, a top level policy on protection of sensitive information may include lower level policies on access control lists (system actions), determining the sensitivity level of information (management processes), and who an employee may discuss the information with (employee actions)
 - Lower level policies may be specific to individual systems
- Multiple levels of a policy may be in a single document, but the development of the complete policy is “**top down**” (bottom-up security won’t work)
- This refinement process level policies may be integrated into the system design process
 - For example, you cannot define a firewall policy until you know your system will use a firewall as enforcement mechanism for a higher level policy
- “High level” and “lower level” policy is not a standard terminology--this is a useful just a way to think about policies

- Security policies are detailed, written documents
 - There are usually multiple documents describing policy on specific areas; e. g., “Internet usage by employees”, “Security patch installation policy”, “Password selection and handling policy” etc.
- Top level policies are often determined by management with significant input from IT: they represent the agency or corporate goals and principals
- It is important that the policies be distributed to those who have to follow the policy and/or implement the policy enforcement method.
- It is critical that employees be **made aware of policies** that affect their actions, violations of which may result in reprimand, suspension, or firing. The fact that individual employees have been made aware should be documented, e. g., by having the employee sign a statement that they attended a training session.
- Every policy must have an enforcement mechanism



Typical elements of the security policy

- Protection of Sensitive Information
 - Addresses the protection goals
 - Defines the way people interact with the data (who gets access, discussing information, printing, storing, etc.)
 - Policy *may* prescribe the technology used to handle sensitive information
 - Audit is usually another enforcement mechanism
- Acceptable Use Policy (AUP) for employee internet access on corporate systems
 - Defines what employees can and cannot use the corporate systems for on the Internet.
 - Should define penalties for violations
 - Policy can state emails sent within the company are not confidential (only business emails are permitted): This allows employer to investigate all email traffic
 - Enforcement: website blocking, activity logging and audit, individual workstation audit

BME Origins of the security policies

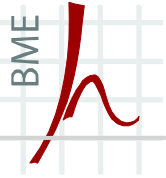
- Broader organizational, corporate or government policies
 - Basics: Virus, worm is not allowed
 - Password basics: Employees should use good passwords. It is not allowed for an employee to grant his/her rights (e.g. password sharing)
 - Etc.
- Risk analysis:
 - Often qualitative (even intuitive) analysis
 - Usually only based on analysis of assets at risk and threats
 - Sensitivity of data (both confidentiality and integrity) is a major source for many organizational level policies, which are based on classes of information → privacy (sensitive data)
 - Vulnerabilities may drive lower level policy
- Concerns about image (corporate, agency, personal)

Inclusive vs. exclusive policy technique

- Inclusive policies explicitly state **what is allowed**, and all other actions are prohibited
 - “Employees may only use the Internet from corporate systems for business related email and web browsing”
 - “Employees may only use the Internet from corporate systems for business related email and web browsing. Occasional personal email and browsing are permitted as long as it does not impact employee performance, corporate system performance and does not include any pornography, illegal activities, or other materials detrimental to the corporation or its perception by the public”
- Exclusive policies explicitly state **what is prohibited**
 - “Employees may not use email or web browsers from corporate systems for personal use.”
 - “Employees may not use email or web browsers from corporate systems for pornography, illegal activities or other materials detrimental to the corporation or its perception by the public
- Similar to default-open, default-closed (N-O, N-C, default deny-default accept etc.) mechanisms firewalls, etc.
- **Inclusive** policies provide automatic prohibition for new applications, technologies, (some) attacks, etc. without changing policy
 - Downloading copyright material for personal use
 - Instant Messaging
- Inclusive policies may need to be updated and updates distributed whenever a new application, technology, etc. comes along

Other policy entries

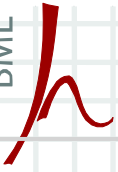
- Employee email usage
- Employee web browsing usage
- Privacy of user information
- Password selection and protection
- Handling of proprietary information
- Cryptographic policy (what needs to be encrypted, what algorithms/implementations/key lengths to use)
- Remote Access
- Protection of employee issued laptops (physical and network connections)
- Configuration Management
- Ongoing Security Monitoring
- Security Patch Management
- Incident Response
- Business Continuity
- Security Audit



A továbbiakban

- Mentés policy: minta: BME szabályzata
- Incidenskezelés
- Munkaköri hatáskörök lásd: IBSZ
- Tűzfalszabályok minta: fw_rules_sample bemutató

- ITB 8. ajánlásból -> más szabványok és eljárásokból táplálkozva
- Informatikai Biztonsági Szabályzat (illetve Informatikai Biztonsági Politika)
- Biztonsági fokozatok
 - alapbiztonság - általános informatikai feldolgozás,
 - fokozott biztonság - szolgálati titok informatikai feldolgozása,
 - kiemelt biztonság - államtitok informatikai feldolgozása.



IBSZ tartalma - *A műszaki-technikai, szakmai védelmi intézkedések*

- Infrastruktúrához kapcsolódó védelmi intézkedések:
 - számítógépet tartalmazó helyiségekbe való belépés rendje,
 - központi gépteremek védelmi előírásai,
 - áramellátás szolgáltatási rendje,
 - telefon kapcsolódás feltételei,
 - tároló-helyiségekre vonatkozó előírások stb.
- Hardverekhez kapcsolódó védelmi intézkedések:
 - kezelési előírások,
 - szállítási rend,
 - felhasználói terminálokra vonatkozó előírások,
 - központi gépekre vonatkozó előírások,
 - speciális biztonsági eszközök alkalmazása stb.

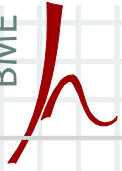
- Adathordozókhoz kapcsolódó védelmi intézkedések:
 - floppyk, mágnesszalagok használatának rendje,
 - biztonsági másolatok készítésének és tárolásának rendje,
 - munkamásolatok készítési és tárolási rendje,
 - adathordozók raktározási, hozzájutási, selejtezési rendje,
 - adathordozók nyilvántartási rendje,
 - titkosítási célra felhasználható adathordozók használata,
 - archiválási rend stb.

- Dokumentumokhoz kapcsolódó védelmi intézkedések:
 - rendszerleírások kezelési, tárolási rendje,
 - rendszerprogram dokumentációk kezelési, tárolási rendje,
 - felhasználói dokumentációk kezelési, tárolási rendje,
 - számítógéppel készített iratok nyilvántartási rendje,
 - automatizált ügyirat kezelés rendje,
 - szerződésben megjelenő adatvédelmi intézkedések,
 - fenti iratok selejtezési rendje stb.

- Szoftverekhez kapcsolódó védelmi intézkedések:
 - rendszerprogramok bevezetésének, használatának rendje,
 - alkalmazói programok bevezetésének rendje,
 - vírusellenőrzési mechanizmus előírása,
 - vírusészleléssel kapcsolatos viselkedési előírások,
 - programtervezési előírások,
 - biztonságot támogató programok használatának rendje,
 - egyéb célú programok használatának rendje stb.

- Adatokhoz kapcsolódó védelmi intézkedések:
 - saját dolgozókról vezetett nyilvántartási előírások,
 - egyéb személyekről vezetett nyilvántartási előírások,
 - adatbeviteli előírások,
 - adat-feldolgozási előírások,
 - adatszolgáltatási előírások,
 - adat kiadmányozási előírások,
 - állandó és ideiglenes adattárolási előírások,
 - adattitkosítási, rejtjelezési előírások stb.
- Kommunikációhoz kapcsolódó védelmi intézkedések:
 - adattovábbítási előírások,
 - adatfogadási előírások,
 - minősített adatok továbbításának rendje,
 - kommunikáció ellenőrzési előírások,
 - "adatszilipelési" előírások stb.

- Személyekhez kapcsolódó védelmi intézkedések:
 - az üzemeltető személyzet feladatai, kötelességei,
 - a rendszergazda feladatai, kötelességei,
 - az adatvédelmi megbízott(ak) feladatai, kötelességei,
 - a karbantartó személyzet viselkedési szabályai,
 - az őrző személyzet kötelességei,
 - a segédszemélyzet feladatai stb.

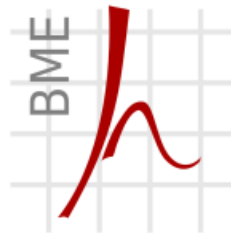


IBSZ - *Eljárási szabályok*

- a riasztó berendezések rendszerbeállításának engedélyezése,
- a rejtjelezéssel kapcsolatos engedélyezési eljárások,
- a nemzetközi adatátvitel eljárási szabályai,
- mágneses adathordozón lévő és vizuálisan nem értelmezhető adatok belföldre, illetve külföldre vitelének ellenőrzési szempontjai,
- a hazai és nemzetközi kapcsolatok létesítésével kapcsolatos külön előírások,
- jogi oltalom alá eső szellemi termékek felhasználásával, forgalmazásával kapcsolatos védelmi szempontok stb.

Kérdések?

KÖSZÖNÖM A FIGYELMET!



Híradástechnikai Tanszék

Dr. Bencsáth Boldizsár
adjunktus
BME Híradástechnikai Tanszék
bencsath@crysys.hit.bme.hu

