Security

Samenvatting

Manuel Mol .

Samenvatting

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aeque doleamus animo, cum corpore dolemus, fieri tamen permagna accessio potest, si aliquod aeternum et infinitum impendere malum nobis opinemur. Quod idem licet transferre in voluptatem, ut postea variari voluptas distinguique possit, augeri amplificarique non possit. At etiam Athenis, ut e patre audiebam facete et urbane Stoicos irridente, statua est in quo a nobis philosophia defensa et collaudata est, cum id, quod maxime placeat, facere possimus, omnis voluptas assumenda est, omnis dolor repellendus. Temporibus autem quibusdam et.

Samenvatting

Published May 24, 2024

Introduction to Information Security

Three important security principles are:

1. Confidentiality: Only authorized users should be able to access data.
2. Integrity: Data should not be altered by unauthorized users.
3. Availability: Data should be available when needed.

AAAA properties:

1. Authenticity: The identity of the user should be verified.
2. Authorization: The user should have the necessary permissions.
3. Accuracy: The data should be accurate.
4. Accountability: The user should be accountable for their actions. (logs)

STRIDE:

1. Spoofing: Pretending to be someone else.
2. Tampering: Altering data.
3. Repudiation: Denying an action.
4. Information Disclosure: Unauthorized access.
5. Denial of Service: Preventing access.
6. Elevation of Privilege: Gaining unauthorized access.

Stride steps

1. Define the key assets and security requirements for the system
2. Design data flow diagram(s) for the system
3. Draw trust boundaries
4. Identify threats
5. Mitigate threats with controls
6. Validate that threats were mitigated

Successful attack:

1. System susceptibility: Vulnerability
2. Threat accessibility: Attack surface
3. Threat capability: recourses, tools, knowledge

Why is security hard?

1. Complexity: More complex systems are harder to secure.
2. Afterthought: Security is often added after the fact.
3. Benefits are evident best after a failure

Security is needed to prevent and counteract the unwanted consequences

Trade-offs:

1. Security vs. Usability
2. Security unaware users want security
3. Security has cost, but becomes only a direct gain when a failure occurs
4. Failure can cost less than prevention
5. Algo is secure but the implementation is not
6. Practical security is ofter weaker than theoretical security

7. Complexity increases the attack surface

Risk management:

Enterprise Risk Management:

1. Identify risks
2. Evaluate risks
3. Mitigate risks
4. Monitor risks
5. Review risks

Risk assessment:

1. Assess risk and determine need
2. Implement policy and controls
3. Promote awareness
4. Monitor and evaluate

Principles, Best Practices and Standards

Design principles:

- Separation of duties: No single person should have all the power
- Least privilege: Only the necessary permissions

Standards and best practices:

- ISO/IEC 27001: Information Security Management System
- NIST: National Institute of Standards and Technology
- ANSI: American National Standards Institute