SECURITY ARCHITECTURE IMPLEMENTATION IN PRACTICE

Marián Illovský
ISACA Slovakia Chapter

2026.06.02.

ISACA®
Budapest Chapter

Security is not a product, but a process – a process that begins with a strong, well-thought-out architecture.“

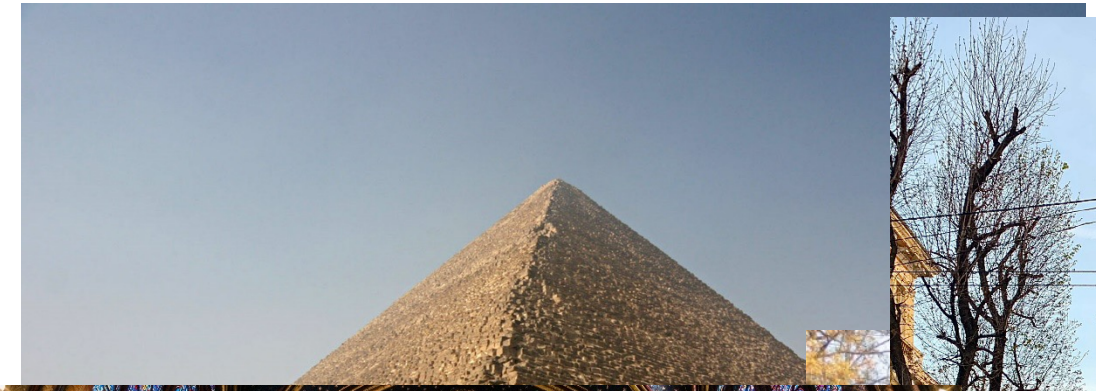
Gary McGraw, software security expert

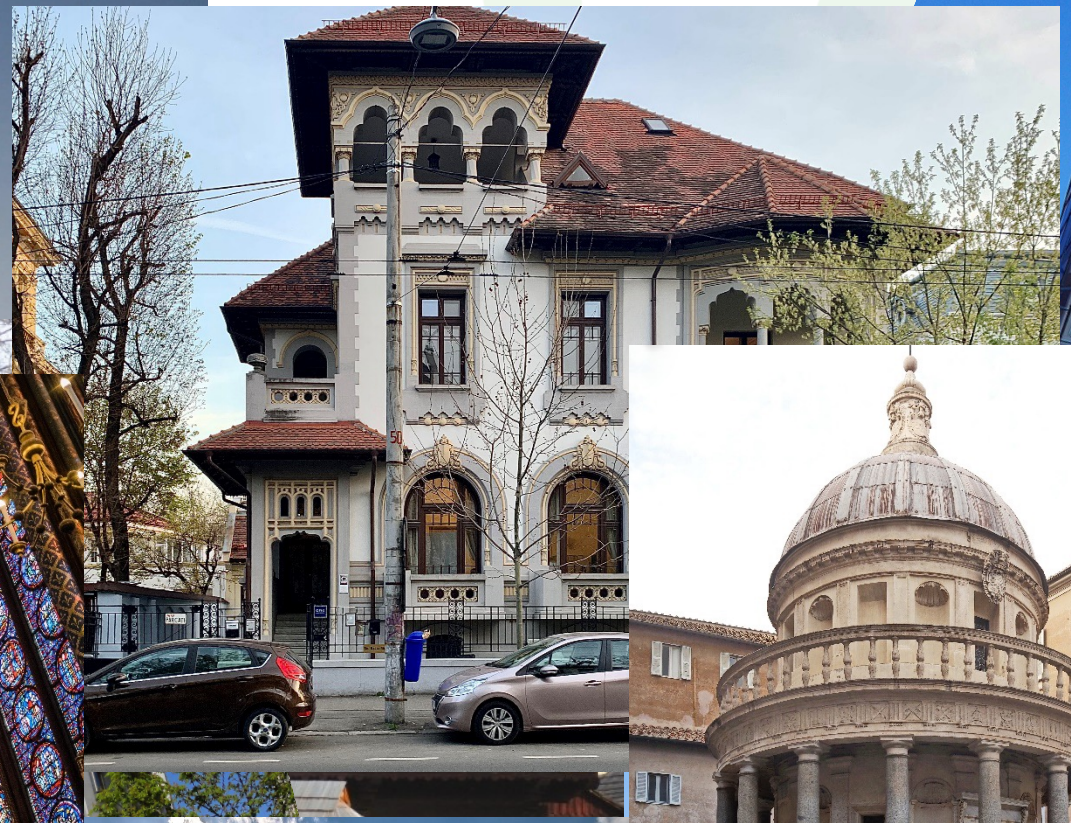
ISACA Budapest Chapter

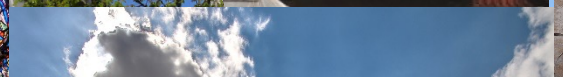
Architecture?

ISACA®
Budapest Chapter

4







And many more architectures...

Landscape Architecture	Garden Architecture	Vehicle Architecture	Process Architecture
Enterprise Architecture	Information Architecture	Technical Architecture	Computer Architecture
HW Architecture	SW Architecture	Zero Trust Architecture	Cloud Architecture

Architecture

- the art and science of **designing and building** structures or systems.
- in a broader sense, it refers to the **deliberate organization** and **arrangement of components** to **create a functional and cohesive whole**.
- Involves **creating a plan or design** that considers the purpose of the structure, **constraints and environment**, so the design is **effective, sustainable, and meets the defined needs**

What does it look like in practice?

ISACA®
Budapest Chapter

Policies, directives, procedures...

ISMS Management Commitment

SEC-PO-001_Security Policy

SEC-SM-001_Security Directive

Physical Security

Procedures for Working in Restricted Areas

Camera System

Access Control System SK

EZS

Dispatch

SEC-PP-003_Personnel Security Process

Non-Disclosure Statement

ISMS Policy and Document Re-training Declaration

Building Information Security Awareness

Information Security with External Parties

SEC-WI-001_Work Instruction for Reception

SEC-F-004_Visitor Rules

Supplier Management Policy

External Developer Management

Screening of Employees

...

Policies, directives, procedures...

...

Human Resources Classification

IT Security Manual

Access Policy and Management

Wifi Networks

Password Policy

GRID Distribution

Operational Procedures for IT

Security Requirements for Camera Monitoring System

Security of Financial Systems

Backup Policy

IT Equipment and Media Disposal Policy

Change Management Policy

Information Transfer Policy

Secure Software Development Policy

Release_Deployment

Security Requirements Analysis in Software Development

Software Product Development and Testing

Vunerability Management

...

Policies, directives, procedures...

...

Antivirus Settings

Hardening guideline

Patch management

SEC-PP-002_Risk Management

Risk Management Methodology

Statement of Applicability

Risks, Threats, and Vulnerabilities

SEC-F-002_Risk register

List of Critical Risks

List of Accepted Risks

Internal Audit of Information Systems

SEC-F-003_Internal Audit Report

Annual Internal Audit Plan

SEC-PP-001_Asset Classification

Working with Classified Information

SEC-F-001_Asset classification

Responsibility Matrix

Incident Management

Clean Desk and Clean Screen Policy

BCM

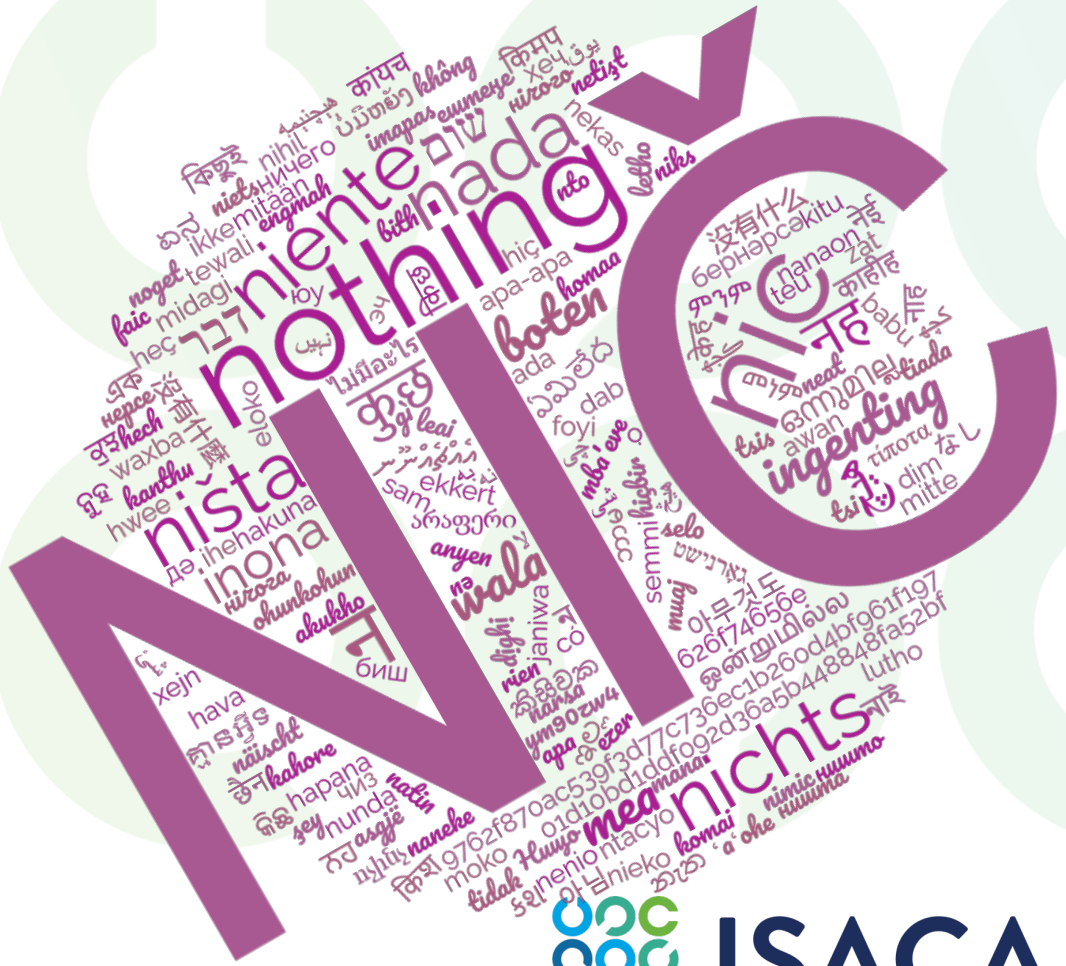
What did you learn from the previous information as a:

Cybersecurity Manager?

CEO?

Auditor?

Regular Employee?



ISACA®
Budapest Chapter

The same, but different

0	1	2	Level 3	Level 4	Level 5	Level 6
ISMS Management Commitment	SEC-PO-001 Security Policy	SEC-SM-001 Security Directive	Physical Security	Procedures for working in restricted areas		
				Camera system		
				Access control system SK		
				Intrusion alarm system (EZS)		
				Dispatch		
			SEC-PP-003 Personnel Security Process	Non-disclosure statement		
				ISMS policies re-training declaration		
				Building information security awareness		
				Information security - external parties		
				SEC-WI-001 Work instruction for reception	SEC-F-004 Visitor Rules	
				Supplier management policy		
				External developer management		
				Employee screening		
				Human resources classification		
			IT Security Manual	Access policy and management	WiFi networks	
					Password policy	GRID Distribution
				Operational procedures for IT	Security requirements for camera monitoring system	
					Security of financial systems	
				Backup policy		
				IT equipment and media disposal policy		
				Change management policy		
				Information transfer policy		
				Secure software development policy	Release Deployment	
					Analysis of security requirements in SW development	
					SW product development and testing	
				Vulnerability management		
				Antivirus settings		
				Hardening guideline		
				Patch management		
				Risk management methodology	Statement of applicability	
					Risks, threats and vulnerabilities	
					SEC-F-002 Risk register	
					List of critical risks / List of accepted risks	
				Internal audit of information systems	SEC-F-003 Internal audit report	
					Annual internal audit plan	
			SEC-PP-001 Asset Classification	Working with classified information		
				SEC-F-001 Asset classification		
			Responsibility matrix			
			Incident management			
			Clean desk and clean screen policy			
			BCM			

ACA®
Chapter

Network Security

We're OK, after all we have:

- 2 firewalls
- 6 switches
- 4 wireless AP
- dedicated serverroom firewall

What did you learn from the previous information as a:

Cybersecurity Manager?

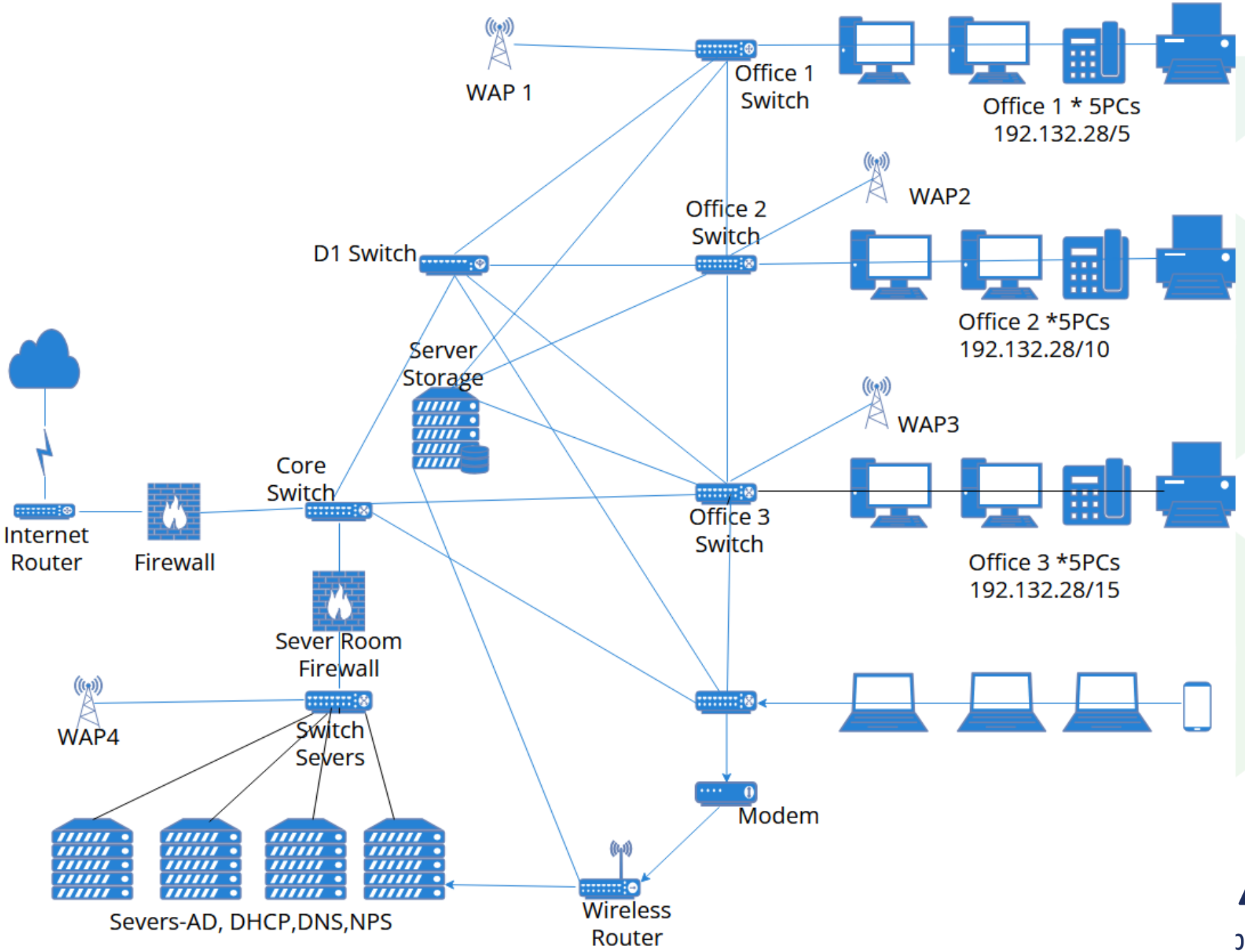
CEO?

Auditor?

Regular Employee?

ISACA®
Budapest Chapter

And suddenly it looks different



ACA
best Chapter

Zero Trust Architecture

„never trust, always verify“

What to do about it?

> An „out of the box“ perspective

> Finding intersections with business

> Defining a „personalized“ security architecture

> Process management / process control

„The only truly secure system is one that is powered off, cast in a block of concrete, and sealed in a lead-lined room with armed guards.“

Gene Spafford, computer security expert

ISACA Budapest Chapter

Questions

ISACA®
Budapest Chapter

Marián Illovský

Board member of ISACA Slovakia chapter

ISACA Budapest Chapter

ISACA®

Budapest Chapter

Thank you!