Pojęcia:

- Data souvereignty
- Confusion – ciphertext differ from plaintext
- Diffusion – zmiana 1 znaku w plaintext = zmiana całego ciphertext
- IRM – Information Rights Management
- DLP
- PII – Personal Identifable Data
- SSN – Social Security Number
- Inbound DLP – emails quarantinne
- Outbound DLP – wire transfer
- Off site recovery – different locations
- CA
- Hot site – duplicate everythng, buy 2 of everything
- Cold site – empty building, no data, no people
- Warm site – between hot & cold
- Honey files – bait, password.txt for example
- Honeypot
- Fake telemetry – niepoprawne (fałszywe) dane, z których są wyciągane jakieś wnioski, na przykład w ML
- DNS sinkhole – celowo kierowany jest złośliwy ruch w inne miejsce (blackhole DNS)
- IaaS =HaaS = CPU, storage, network, BRAK: OS
- SaaS
- PaaS – no servers, no software, no maintenance team, you have platform to create an app, building blocks
- XaaS – Anything as a Service
- On premise – u nas
- Off premise – your servers not in your building, specialized provider
- Edge computing – data processed on local system, no latency, process where data is
- Fog computing -cloud that's close to your data, long-term analysis in cloud, private data never send
- Thin client – dostarcza tylko tyle mocy żeby połączyć się do virtual desktop in the cloud
    - Good connectivity needed
- In client-server model, the term "Thin client" refers to a networked computer equipped with the minimum amount of hardware and software components. As opposed to thick client, which runs applications locally from its own hard drive, thin client relies on network resources provided by a remote server performing most of the data processing and storage functions.
- Virtualization
- Hypervisor
- Container
- Microservices
- API Gateway - an application programming interface (API) gateway is software that takes an application user's request, routes it to one or more backend services, gathers the appropriate data and delivers it to the user in a single, combined package
- Serverless architecture – FaaS – Function as a Service
- Transit gateway – cloud router

- Vm sprawl avoidance – trzeba unikać niekontrolowanego rozrostu puli maszyn wirtualnych
- Sandbox
- Orchestration
- Stored procedures – created on database
- Obfuscation
- Code reuse
- Dead code – kod w aplikacji, który nie jest wykorzystywany
- Mirror site
- Federation – logowanie przez providera (za pomocą FB lub twittera na przykład)
- Attestation – prove that hardware is really yours, send report
- Smard card = chip
    - example implementation of certificate-based authentication
- Retinal – tył oka
- Gait analysis – sposób chodzenia
- Multipath I/O
    - "Multipath I/O" refers to a framework that improves fault tolerance and performance by enabling additional, alternate routes for data that is being transferred to and from storage devices.
    -
- NIC teaming – multiple network interface cards
    - The process of combining multiple physical network adapters into a single logical interface for increased throughput and redundancy is called
- Generator – long term power backup
- Hot-swappable – replace faulty power supply without powering down
- Archive attribute
- Magnetic tape/disk
    - sequential-access backup media
- Offline / online backup
- Non-persistence
- Surveillance systems – nadzór
- Barricades / bollards
- Alarms
    - Circuit-based
    - Duress (panic button)
    - Motion detector
- USB data blocker – prevent juice jacking
- Juice jacking – pobieranie danych po USB
- File supression:
    - Dupont
    - FM-200
- Screened subnet = DMZ = perimeter network
- Air gap – separacja sieci
    - Method of isolating computer or network from internal/external network
- Vault/safe
- Hot and cold aisle
- Obfuscation / code obfuscation
- Security throught obscurity

- Qbit – between 1 and 0, 1 and 0 at the same time
- Blockchain
- API gateway
- Modele finansowania:
    - On-prem = CAPEX
    - Cloud = OPEX
- Applications Delivery Services – kontener aplikacji wysyłany do klienta
- Terminal services – app runs on the server and video is being streamed
- ESX runs on a bare metal
- Staging = preprod
- 3 pass wipe needed
- Secure boot – list of apps anchored to TPM
- Normalization – database integrity & optimization
    - Data normalization ensures that attributes in a database table depend only on the primary key. Normalization is required to prevent repetitive information from appearing in database.
- Software diversity – kod inny, funkcje te same
- One-way trust: A trusts B, B doesn't trust A
- Two-way trust
- Transitive trust: A trusts B, B trust C = A trusts C
- Non-transitive trust
- Attestation – prove that system is secure and operates from secure code base (TPM)
- Static codes – dużo kodów pojedynczego użytku
- Live boot media – removable storage media that contains portable, non-persistent OS
- Bollard
- Jersey barrier – te biało-czerwone na drodze
- Man-trap – śluza
- Badge
- Locking cabinets – zamykane szafki
- Emanations / FM frequencies – podsłuchiwanie sieci za pomocą np. fal
- DMZ = screened subnet = perimeter network
- Alarmed carrier – monitor for vibrations associated with attempted access
- Continuously view carrier – guards
- Faraday cage – protect against EMI, RFI

Skrótowce:

- MSP – Managed Service Provider – network connectivity, backups, growth (outsourced IT)
- MSSP – Managed Security Service Provider
- VDI – Virtual Desktop Infrastructure
- DaaS – Desktop as a Service (VDI)
- FaaS – Function as a Service
- VPC – Virtual Private Cloud
    - Pool of resources in public cloud
- SIAM – Service Integration and Management
    - Many different service providers, every provider work different
- SDN – Software Delivery Network

    - Control / data plane
- SDV – Software Defined Visibility
- VXLAN – Virtual Extensible LAN
- QA – Quality Assurance,
    - sprawdzają, czy są wymagane funkcje
- CI – Continous Integration
    - code is constantly written and merged into repository
- CD – Continous Delivery/ Deployment
    - release process automated (PROD)
- SMS – Short Message Service
- HOTP – HMAC-based One Time Password
    - Valid for only one login session
    - Based on a cryptographic hash function and a secret cryptographic key
    - Not vulnerable to replay attacks
- FAR – False Acceptance Rate
- FRR – False Rejection Rate
- CER – Crossover Error Rate, FAR = FRR
- AAA – Authentication, Authorization, Accounting
    - Accounting - login time, logon time
- RAID – Redundant Array of Independent Disks
    - A dedicated data storage solution that combines multiple disk drive components into a single logical unit to increase volume size, performance, or reliability
- LBFO – Load Balancing / Fail Over
    - 2 karty NIC połączone switchem
- UPS – Uninterruptible Power Supply
    - Offline/standby UPS – not normally enabled unless power is lost
    - Line-interactive UPS – stopniowo redukuje różnicę w opadającym napięciu
    - On-line/double conversion – działa zawsze
    - provide short-term emergency power during an unexpected main power source outage
- PDU – Power Distribution Unit
    - Provide multiple power outlets (control & monitor)
    - device designed to distribute (and monitor the quality of) electric power to multiple outlets
- SoC – System on a Chip
    - Multiple functions, embedded systems
- FPGA – Field-Programmable Gate Array
    - Can be configured after manufacturing
    - Array of logic blocks
- SCADA – Supervisory Control and Data Acquision System
    - Large scale, multi-site industrial control systems (ICS)
- ICS - Industrial Control Systems
- VoIP – Voice over IP
- POTS – Plain Old Telephony System
- HVAC – Heating, Ventilating, Air Conditioning
- MFD – Multi Function Device
    - Printer, scanner

- MFP – Multi Function Printer
- RTOS – Real Time OS
- CCTV – Closed Circuit TV
- PDS – Protected Distribution System
    - Bezpieczne kable
- HE – Hommomorphic Encryption
    - Perform operations on data while are encrypted
- ECC – Eliptic Curve Crypto
    - perfect for mobiles (asymmetric)
- NTRU
    - Nie rozwijany skrót
    - Encryption with quantum-computing, “closest vector” problem
- QKD – Quantum Key Distribution
- PFS – Perfect Forward Secrecy
- IPAM – IP Address Management
- NAT – Network Address Translation
    - Hide private IP
- PAN – Primary Account Number
- PAN – Personal Area Network
- HVT – High Value Token
    - Credit cards, PAN
- LVT – Low Value Token
- DRM – Digital Rights Management
- TPM – Trusted Platform Module
- HSM – Hardware Security Module
    - Removable or external
- CASB – Cloud Access Security Broker
    - Between company and cloud provider
    - Functions as: logging, SSO
- IaC – Infrastructure as a Code
- MOP – Methods of Operation
- ROTS – Root of Trust
- PIV – Personal Identification Verification card
- CAC - Common Access Card
- DoD - Department of Defense
- HBA – Host Bus Adapter
    - Like a NIC
- RPO – Recovery Point Objective
- RTO – Recovery Time Objective
- SLA – Service Level Agreement
- PSTN – Public Switched Telephone Network
- POTS – Plain Old Telephone System
- SPIT – Spam over Internet Telephony
- PBX – Private Branch Exchange
    - Internal telephone exchange or switching system, allows internal communication
    - VoIP
- SoC – System on a Chip

    - Raspberry PI, mobile
- TPI – Two Person Integrity
- RNG / PRNG / QRNG - Quantum

Niszczenie dysków

- Pulverizer – rozdrabnianie
- Degaussing – electromagnetic
- Incineration – spopielanie
- Purge data = delete
- Wipe data = unrecoverable removal
- Sdelete – file level overwrite
- DBAN – whole drive wipe

MFA factor:

- something you know
- something you have
- something you are

MFA attributes:

- inne

SAN I NAS:

NAS – Network Attached Storage	File level access	Shared storage device across network • dedicated storage appliance that can be added to a local network
SAN – Storage Area Network	Block level access – can change only portion of file	Feels like local storage device • dedicated local network consisting of devices providing data access

Typy backup'ów:

Type	Backup speed	Restore speed	Features
Full backup	High	Low	
Incremental backup	Low	High (multiple sets)	All files changed since last incremental backup
Differential backup	Moderate	Moderate (no more than 2 sets)	All files changed since last full backup

RAID (rajdy):

RAID level	Required number disks to implement	Possible failure	Features
RAID 0	2	0	No fault tolerance, high performance
RAID 1	2	1	Mirroring
RAID 5	3	1	Stripping + parity
RAID 6	4	2	Stripping + 2 parity
RAID 10	4	1~2	Stripping + mirroring

RAID level	More features
0	Requires a minimum of 2 drives to implement Is also known as disk striping Decreases reliability (failure of any disk in the array destroys the entire array) Is suitable for systems where performance has higher priority than fault tolerance

Komunikacja:

- Narrowband – narrow range of frequencies, longer distance
- Boradband – wider frequencies, less power ~~and distance~~
- Baseband – single frequency, single cable, utilization 0% or 100%
    - 100 Base-TX
- Zigbee – alternative to WiFI / BLE, longer distance, less power consumption (ISM band)
    - IoT technology designed to provide communication between appliances in a home automation network
    - Very short range, used in house

Wejściówki / karty wejściowe itp:

- ID badge – picture, name
- RFID badge
    - Proximity card
- PIV – Personal Identification Verification card
    - US Federal smard card
- Common Access Card
    - Department of Defense
- Proximity reader – NFC lub RFID chip
-

Kryptografia:

- Cryptoanalysis – łamanie szyfrów

- the field of data security, the term "Tokenization" refers to the process of replacing sensitive data with nonsensitive information which holds a reference to the original data and enables its processing but has no value when breached.
- Key stretching/strengthening – hash of a hash of a hash (weak key)
- Bcrypt – extension to UNIX crypt library, blowfish cipher to perform multiple rounds of hashing
- PBKDF2 – part of RSA (key stretch), bcrypt, blowfish
- Lightweight crypto – na urządzeniach IoT, pewnie też na mobiles
- HE – Hommomorphic Encryption
    - Perform operations on data while are encrypted
- Symmetric encryption – secret key crypto
- Asymmetric encryption – public key crypto
- Digital signature – Authentication, No-repudiation, Integrity
- Symmetric key = B priv K + A pub K = A priv K + B pub K (DIFFIE HELLMAN KEY EXCHANGE)
- ECC – Eliptic Curve Crypto – perfect for mobiles (asymmetric)
- Assymetric keys – common length of >3k bits
- Out-of-band key exchange – pocztą na przykład
- In-band exchange – use symmetric encryption
- Session key = symmetric key = private key
- ephemeral key = asymmetric key
- PFS – Perfect Forward Secrecy
    - Don’t use server’s private RSA key
    - Eliptic curve or D-H ephemeral
    - Every session use another key
    - Require more computing power
    - Session key derived from set of long-term keys, long term key compromised != session key compromised
- Stream cipher I block cipher to są symetryczne algorytmy
- ECB – Electronic Code Book – the same encryption for all
- CBC – Cipher Block Chaining – plaintext XOR with previous ciphertext
- CTR – Counter mode – plaintext XOR with key + counter
- GCM – Galois / Counter mode – commonly used in TLS, IPSec
- Hashing – data integrity
-
- Vigenere table – podstawienia: key word & message

Symmetric ciphers	Asymmetric ciphers
RC4, RC5	RSA
DES, AES, 3DES	GPG, PGP
Blowfish, Two-fish	DHE, ECDHE
IDEA	DSA
Skipjack	Elgamal
	ECC
	Diffie hellman