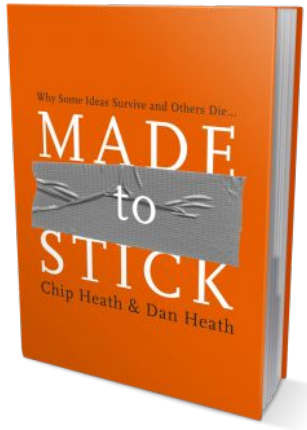
Group 7 – Virtualization

Cryptography & Network Security

BTech ETT (Year 4, ULK)

Learning Objectives

- Understand virtualization in telecom & IT
- Types: server, network, storage
- Know risks & security issues
- Plan disaster recovery & incident response
- Apply to real-world companies



Case Description

- Small & medium businesses need reliable IT at low cost
- Use virtualization (VMs & containers) instead of many servers

➔ **Benefits**

cost-effective, easy to expand, fast to manage.

➔ **Risks**

hypervisor attacks, VM sprawl, data leakage.

Types of Virtualization

1. **Server**: Many OS on one machine (KVM, VMware)
2. **Network**: Software replaces firewalls, routers (NFV)
3. **Storage**: Combine devices into one logical system
4. Example: running VPN, firewall, core services as VMs

Security Concerns

1. Hypervisor attacks → patch & harden
2. VM sprawl → manage lifecycle
3. Shared resources → segmentation & encryption
4. Insider threats → RBAC & MFA

Disaster Recovery Plan

1. Regular backups (VM snapshots)
2. Redundancy across sites
3. Failover to other servers
4. Regular testing & drills

Incident Response Plan

- Detect → monitor logs
- Contain → isolate VMs
- Eradicate → remove threat & patch
- Recover → restore clean backups
- Learn → improve policies

Discussion Questions

1. Benefits of virtualization in telecom?
2. Risks vs physical systems?
3. How to secure hypervisors?
4. VM vs container – which is better?
5. How does DR change with virtualization?

Conclusion

- Virtualization saves cost, adds flexibility, and speed
- New risks must be managed
- Security, DR, and incident response are essential
- With good planning, companies gain more benefits than risks