🛡️ IT Security Policy Framework

Mapping to the Seven Domains

Because security without documentation is just expensive paranoia 📚

🎯 The Seven Domains Overview

1. **User Domain** 👥
2. **Workstation Domain** 💻
3. **LAN Domain** 🌐
4. **LAN-to-WAN Domain** 🌍
5. **WAN Domain** ☁️
6. **Remote Access Domain** 🔗
7. **System/Application Domain** 🖥️

🧠 "I know all seven domains!"

💭 *Forgets which domain the printer belongs to*

👥 Domain 1: User Domain

Policy Framework Mapping

Key Policies:

- Acceptable Use Policy (AUP)
- Password Policy
- Security Awareness Training
- Incident Reporting

📊 **Case Study: Phishing Nightmare at MegaCorp**

Employee clicked malicious email → Compromised credentials → $2.4M data breach

Solution: Implemented mandatory phishing simulation training + strict email filtering policies

👤 User: "My password is 'password123'"

🔒 IT Security: "That's not secure!"

👤 User: "Fine, 'Password123!'"

🤦 IT Security: *internal screaming*

💻 Domain 2: Workstation Domain

Policy Framework Mapping

Key Policies:

- Endpoint Security Policy
- Software Installation Policy
- Patch Management Policy
- Device Configuration Standards

📊 Case Study: The USB Stick Disaster

Finance employee found USB in parking lot → Plugged into work computer → Ransomware infected entire finance network

Solution: USB port blocking policy + employee education on social engineering

💾 "Found this USB in the parking lot!"

🔌 *Immediately plugs it in*

💥 **RANSOMWARE DEPLOYED**

😱 "Why is everything encrypted?"

🌐 Domain 3: LAN Domain

Policy Framework Mapping

Key Policies:

- Network Segmentation Policy
- VLAN Management Policy
- Switch Configuration Standards
- Network Access Control (NAC)

📊 Case Study: The Printer That Saw Everything

Unsecured network printer → Lateral movement → Access to financial systems

Solution: Network segmentation + IoT device isolation policies

🖨️ Smart Printer: "I can scan, print, fax, AND spy on your network!"

🌐 Network Admin: "Wait, what was that last part?"

🖨️ Smart Printer: "...make copies?"

🤔 Network Admin: "Suspicious..."

🌍 Domain 4: LAN-to-WAN Domain

Policy Framework Mapping

Key Policies:

- Firewall Management Policy
- DMZ Configuration Policy
- Intrusion Detection/Prevention Policy
- Traffic Monitoring Policy

📊 **Case Study: The Misconfigured Firewall**

"Any-Any-Allow" rule left active → Direct internet access to internal servers → SQL injection attack

Solution: Firewall rule review policy + change management procedures

🔥 Firewall: "SHALL NOT PASS!"

💻 Hacker: "What about through port 80?"

🔥 Firewall: "Oh, that's fine, come on through!"

🤦 Network Admin: "I may have misconfigured something..."

☁️ Domain 5: WAN Domain

Policy Framework Mapping

Key Policies:

- Internet Usage Policy
- Cloud Service Provider Policy
- Bandwidth Management Policy
- Third-Party Connection Policy

📊 **Case Study: Shadow IT Strikes Back**

Marketing team used unauthorized cloud storage → Sensitive data leaked via public sharing link

Solution: Cloud Access Security Broker (CASB) + approved cloud services policy

☁️ "Let's just use this free cloud service!"

📊 *Uploads entire customer database*

🌍 *Link accidentally shared publicly*

📰 "Company X leaks 50,000 customer records"

😭 "Oops..."

🔗 Domain 6: Remote Access Domain

Policy Framework Mapping

Key Policies:

- VPN Access Policy
- Remote Work Policy
- Multi-Factor Authentication Policy
- Mobile Device Management (MDM)

📊 **Case Study: Coffee Shop Catastrophe**

Executive used public Wi-Fi for VPN → Man-in-the-middle attack → Credentials compromised

Solution: Always-on VPN policy + public Wi-Fi usage restrictions

☕ Working from coffee shop...

📶 "FreeWiFi" looks legit!

🔓 No VPN needed, right?

👩‍💻 Hacker: "Thanks for the login credentials!"

😨 "Why is someone in Kazakhstan accessing our servers?"

💻 Domain 7: System/Application Domain

Policy Framework Mapping

Key Policies:

- Application Security Policy
- Database Security Policy
- Server Hardening Standards
- Backup and Recovery Policy

📊 **Case Study: The Default Password Debacle**

New application deployed with default admin credentials → Discovered by automated scanners → Complete system compromise

Solution: Secure deployment checklist + credential management policy

🔧 "Just deployed the new system!"

🔑 Password: admin/admin

💭 "I'll change it later..."

🤖 *Bot scans internet*

💥 "System compromised in 3... 2... 1..."

😵 "Later never came..."

📋 Policy Documentation Best Practices

Essential Documentation Components

- **Purpose & Scope -** Why does this policy exist?
- **Roles & Responsibilities -** Who does what?
- **Compliance Requirements -** Legal/regulatory obligations
- **Implementation Guidelines -** How to actually do it
- **Monitoring & Enforcement -** Consequences and auditing

📚 Policy Document: 247 pages

👨‍💼 Employee: "TL;DR version?"

📄 IT: "Don't click suspicious links"

👨‍💼 Employee: "Got it!"

📧 *Immediately clicks phishing email*

🔄 Cross-Domain Policy Integration

The Domino Effect

- User clicks malicious link (**User Domain**)
- Workstation gets infected (**Workstation Domain**)
- Malware spreads through network (**LAN Domain**)
- Breaches firewall (**LAN-to-WAN Domain**)
- Exfiltrates data to internet (**WAN Domain**)
- Compromises VPN users (**Remote Access Domain**)
- Attacks critical applications (**System/Application Domain**)

🎯 "It's just one small security gap..."

⛓️ *Chain reaction begins*

💥 "EVERYTHING IS ON FIRE!"

🔥 "This is fine" dog meme energy

📊 Real-World Implementation Stats

Policy Effectiveness Metrics

- **95%** reduction in security incidents with proper user training
- **80%** fewer breaches with network segmentation
- **67%** faster incident response with documented procedures
- **45%** cost reduction through standardized policies

📊 **Success Story: TechStart Inc.**

Implemented comprehensive 7-domain policy framework → Zero major security incidents in 18 months → Achieved SOC 2 compliance → Won major enterprise contracts

🚨 Common Policy Pitfalls

The "Swiss Cheese" Model

- Policies with gaps = Multiple failure points
- No regular updates = Outdated protections
- Poor documentation = Confused implementation
- Lack of training = User non-compliance

🧀 Security Policy: "We have holes, but we're still cheese!"

🐭 Threat Actor: "Perfect, I love cheese!"

🧀 Security Policy: "Wait, that's not how this works..."

🐭 Threat Actor: *Already inside the network*

🎯 Implementation Roadmap

Phase 1: Foundation (Months 1-3)

- Document current state
- Identify critical gaps
- Develop core policies

Phase 2: Deployment (Months 4-6)

- Roll out policies by domain
- Conduct training sessions
- Implement monitoring

Phase 3: Optimization (Months 7-12)

- Regular reviews and updates
- Incident response testing
- Continuous improvement

🏆 Success Metrics & KPIs

What to Measure

- **Incident Response Time**: < 4 hours to containment
- **Policy Compliance Rate**: > 95% adherence
- **Training Completion**: 100% of users annually
- **Vulnerability Remediation**: < 30 days for critical issues

📈 "Our security metrics are improving!"

📊 *Shows beautiful dashboard*

💥 *Major breach happens next day*

📉 "Metrics don't lie, but timing does..."

🔧 Tools & Resources

Documentation Tools

- **Policy Templates**: NIST, ISO 27001 frameworks
- **Collaboration Platforms**: SharePoint, Confluence
- **Version Control**: Git for policy versioning
- **Training Platforms**: KnowBe4, SANS Security Awareness

Monitoring & Compliance

- **SIEM Solutions**: Splunk, QRadar, ELK Stack
- **Vulnerability Scanners**: Nessus, OpenVAS
- **Compliance Tools**: Rapid7, Qualys VMDR

💡 Key Takeaways

1. **Holistic Approach**: All seven domains are interconnected
2. **Living Documents**: Policies must evolve with threats
3. **User Education**: Technical controls + human awareness
4. **Regular Testing**: Policies are only as good as their implementation
5. **Continuous Improvement**: Security is a journey, not a destination

🎓 "I've read all the security policies!"

📚 *Stack of 500+ pages*

🧠 "I understand everything!"

📧 *Gets phished 5 minutes later*

🤡 "Theory vs. Reality: The Eternal Struggle"

🚀 Questions & Discussion

Think About

- Which domain poses the biggest risk in your organization?
- How do you ensure policy compliance without being the "security police"?
- What's your experience with cross-domain security incidents?

🤔 "Any questions about IT security policies?"

🤦 "Yeah, can we just not have them?"

🛡️ "That's... not how security works..."

🤦 "But they're so complicated!"

📈 *Breach statistics intensify*

📚 Additional Resources

Standards & Frameworks

- **NIST Cybersecurity Framework**
- **ISO 27001/27002**
- **COBIT 2019**
- **SANS Critical Security Controls**

Documentation Templates

- Policy template libraries
- Incident response playbooks
- Risk assessment matrices
- Compliance checklists

Remember: Good documentation today prevents tomorrow's "How did this happen?" meetings! 🎯