Protecting Your Network

Jörg Maaß

Senior Product Manager Security

Agenda

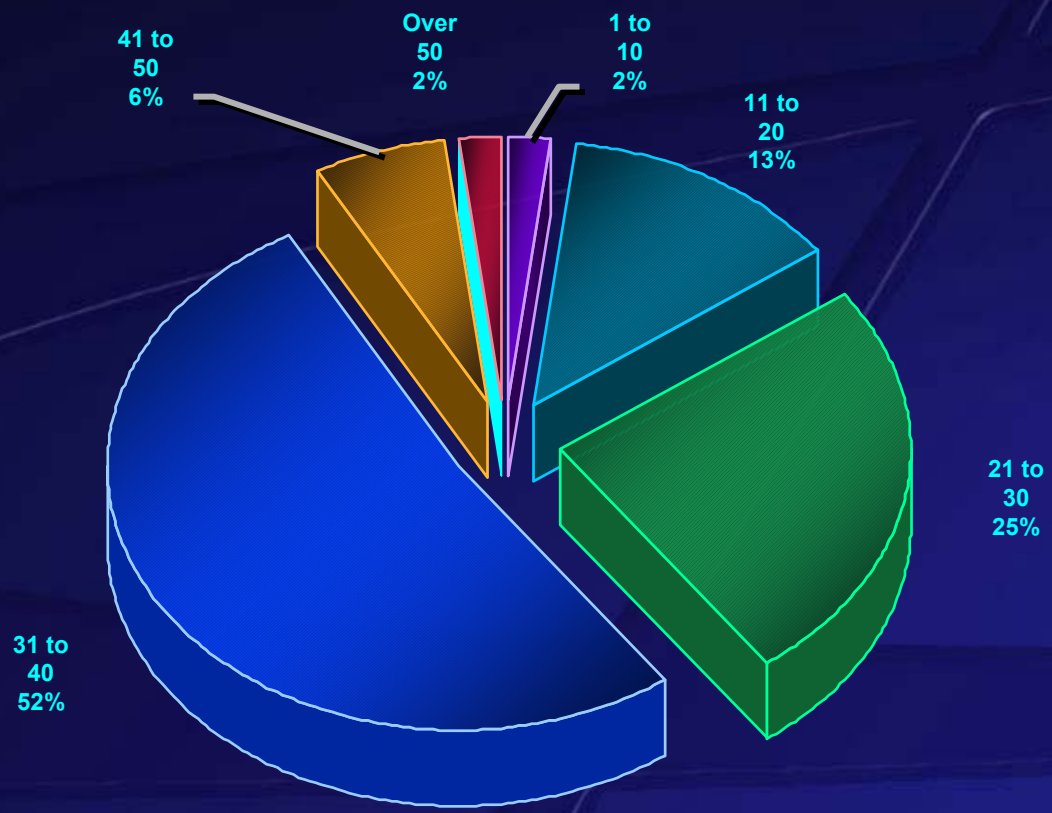
- Facts on Security
- Types of Threats
- The Legal Situation
- Security is a Corporate Function
- Risk Assessments and Audits
- Methods of Detection
- Methods of Protection
- Methods of Analysis and Forensics
- KPNQwest as a Security Provider

Threats and Facts

- 70 % of surveyed companies suffered security breaches
  - 59% attacks from outside
  - 38% attacks from inside
  - 74% suffered financial loss
- Source of the attack
  - Foreign Governments: 21%
  - Foreign Corporations: 30%
  - Independent Hackers: 77%
  - US Competitors: 44%
  - Disgruntled Employees: 81%

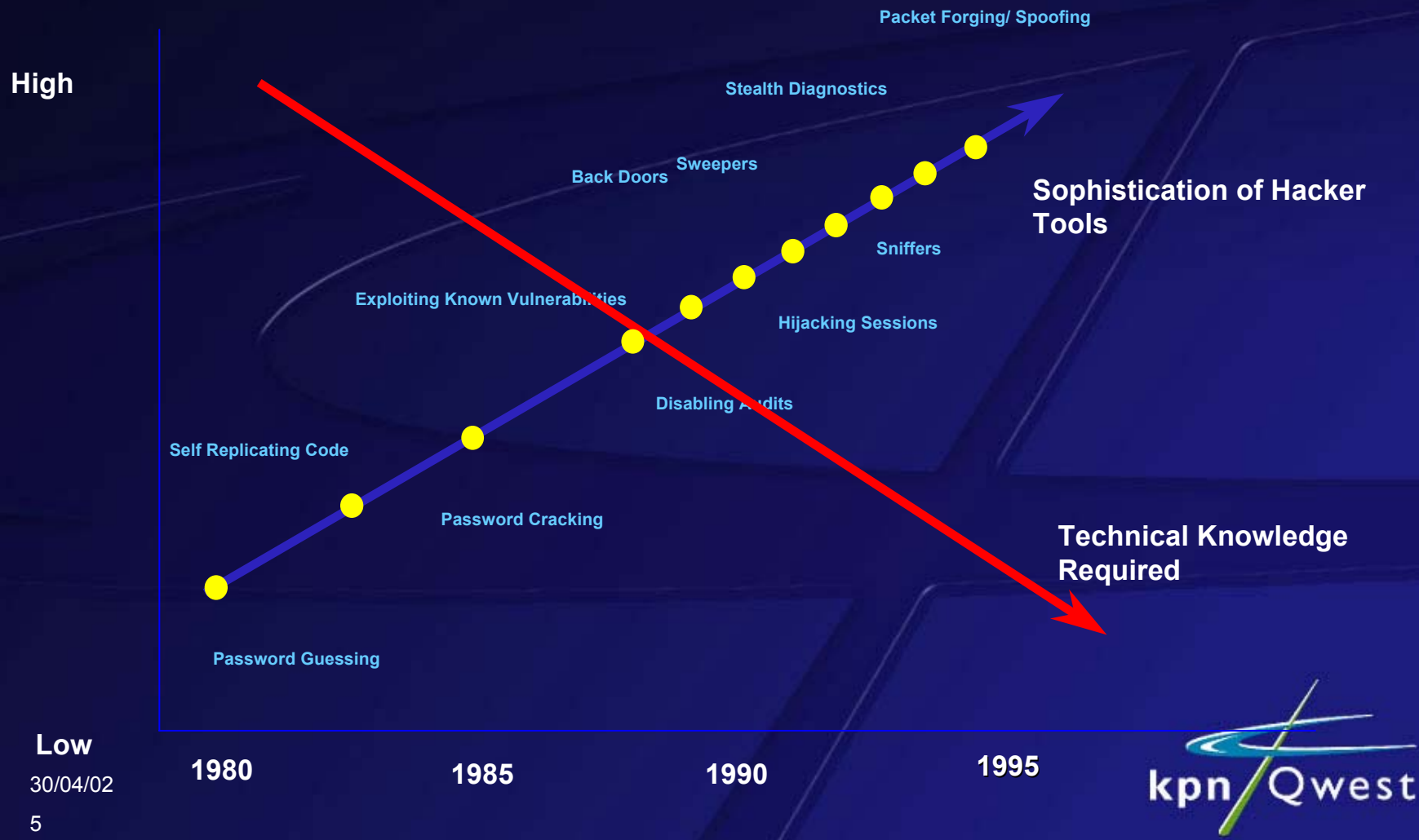
60 % penetrated 30 Times

Over the Past 12 Months, How Many Successful Unauthorised Accesses from Outsiders Have You Detected?



Source: WarRoom Research, Internet Week, 23 March 1998

Threat Capabilities

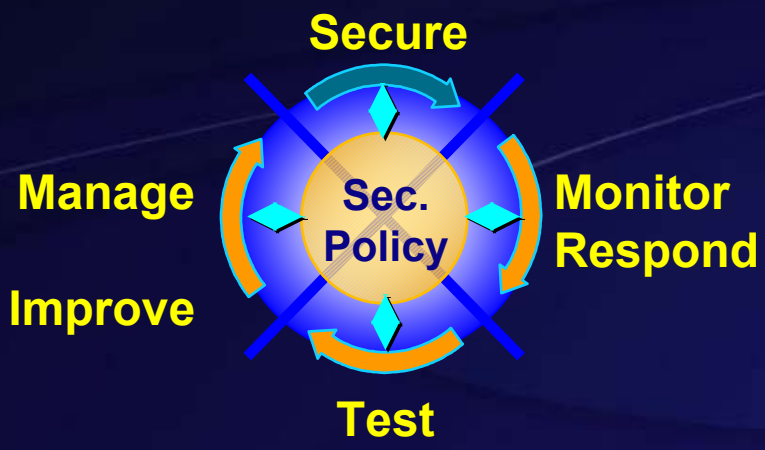


The Legal Situation

- New Cyber Crime legislation by the European Council
- Corporate Management is legal representative of the Corporation and directly and personally responsible for
  - Computer Crimes committed by them
  - Computer Crimes committed by employees
  - Lack of Control and Oversight of security relevant actions and operations
- Security Risks that involve financial risk to the Corporation need to be included in Corporate Reports
- Legal situation differs from country to country

kpn Qwest

Security is a Corporate Function



- Proper security organisation and processes are important
- Security is a cross functional business component
- Security is a matter for the boss
- Security Policy is first start
- Valuable assets are then analysed and tested for risks
- Security is a process that requires constant attention

kpn Qwest

Organisational Measures

- Create senior management awareness and support
  - FUD Tactics won't help in most cases
  - Concentrate on benefits: customer trust and loyalty, less downtime, no loss of reputation
- Establishment of Security Officer
- Definition of Corporate Security Policy
- Concentration on key areas
  - Extranet, Remote Access
  - Corporate Website, Key Applications
- Security Assessment: Analysis of existing infrastructure
- Security Concept: What to change, how and when
- Implementation

kpn Qwest

Methods of Detection

- Constant Vigilance and Sensitisation for Security
- Monitoring of your infrastructure
- Regular Security Audits
- Security Processes
- RMON Probes
- Intrusion Detection Systems
- File System Integrity Checks
- Physical Access Control
- Analysis of Log Files

kpn Qwest

Methods of Protection

- Common Sense
- Constant Vigilance and Sensitisation for Security
- Mandatory Process Checkpoints
- Regular Security Audits
- Security Processes
- Password Policy
- Physical Security
- Firewalls
- Anti Virus SW, Active Content Screening
- URL Filtering
- Advanced Authentication (Token Cards, Certificates)

kpn Qwest

Forensics or “Deep Impact”

- Do we want to prosecute an alleged computer crime?
- If in doubt, leave forensics to the experts!
- Secure possible evidence
- Responsible person should not be involved in any way
- Have one person responsible
  - Evidence Collection
  - Co-ordination
  - Interfacing to outside entities
- All handling of potential evidence must be documented
- Differing requirements of evidence handling per country
- Contact Authorities proactively
- Expect lengthy and often “mysterious” process

kpn Qwest

KPNQwest as a Security Provider

- European Provider of Business Infrastructure and Services
- Present in 18 European Countries, North America and Asia (through Qwest)
- Managed Firewall Service
- Self-Managed Firewall
- Advanced Security Solutions such as Anti Virus, URL Blocking, Intrusion Detection, Advanced Authentication
- Technical Security Consulting
- Secure Hosting Centres (CyberCentre)