Chapitre 1

Sommaire

IT Security Timeline

1969	1975	1977	1979	1982	1983	1985	1986	1988	1989	1990
First message sent via ARPANET ISACA founded	First test of TCP/ IP between two networks	Apple II	FFIEC	Commodore 64	ARPANET migrated to TCP/IP "WarGames"	Windows 1.0	Computer Fraud and Abuse Act	Morris worm → CERT	SANS Institute founded $(ISC)^2$ founded "Cuckoo's Egg"	ARPANE decommis-sioned → Internet born HTTP, HTML, first web server, first web browser

1992	1993	1994	1995	1996	1999	2000	2001	2002	2003	2004
Michelangelo virus "Sneakers"	First DEF CON conference SAS 70	CISSP credential-launched Vladimir Levin hacks Citibank	SSL BS 7799	High-profile website de-facements (CIA, USAF, etc.) HIPAA COBIT	Melissa virus Back Orifice 2000 GLBA	ILOVEYOU worm	NIST chooses AES First major DDoS attack involving DNS servers as reflectors Code Red worm	FISMA Sarbanes-Oxley California enacts first data breach-notification law	National Cyber Security Division opens within Dept. of Homeland Security Anonymous formed	PCI DSS

2005	2006	2007	2008	2009	2010	2011	2012	2014	2015	
NIST SP 800-53 ISO/IEC 27001 TJX hacked	VA loses laptop containing data on 26.6 veterans and families 21,549 sites defaced at once by single hacker	Successful spear phishing attack of Office of Secretary of Defense Country of Estonia suffers 22-day DDoS attack	Cloud Security Alliance	Conficker worm FAA hacked HITECH	Stuxnet worm US Cyber Command activated	FedRAMP SSAE 16/ SOC 2 Bank of America hacked PlayStation Network hacked Reported hacks of DoD, Pentagon, NASA, etc. 700,000 websites defaced at once by single hacker	Marriott hacked Farmers Insurance hacked Mastercard hacked SCADA systems of 6 countries including US hacked	OPM hacked Target hacked Sony hacked Home Depot hacked US Postal Service hacked	White House hacked Anthem hacked Pentagon hacked IRS hacked United Airlines hacked CIA Director's email hacked SSL officially replaced by TLS 1.2	

Trends:

- Attacks: more sophisticated, frequent, and successful
- Need for security professionals increasing: regulatory requirements, business self-protection, customer demands, etc.

Legend:

- Technology
- Hacks, Attacks, and Data Breaches
- Laws, Rules, Standards, and Regulations
- Certifications and Organizations

Section 1.1: Sécurisation des réseaux

À la fin de cette section, vous devriez pouvoir :

- Décrire le paysage actuel de la sécurité réseau.
- Expliquer comment tous les types de réseaux doivent être protégés.

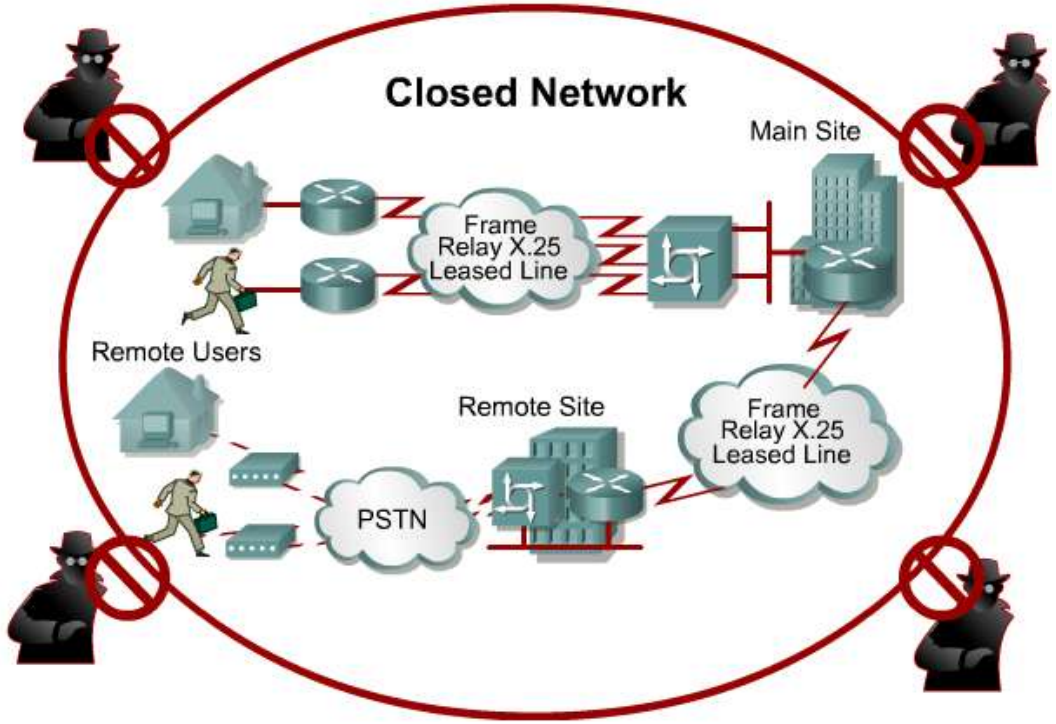
1.1.1Situation actuelle

Les réseaux sont des cibles

Source : **map.norsecorp.com**

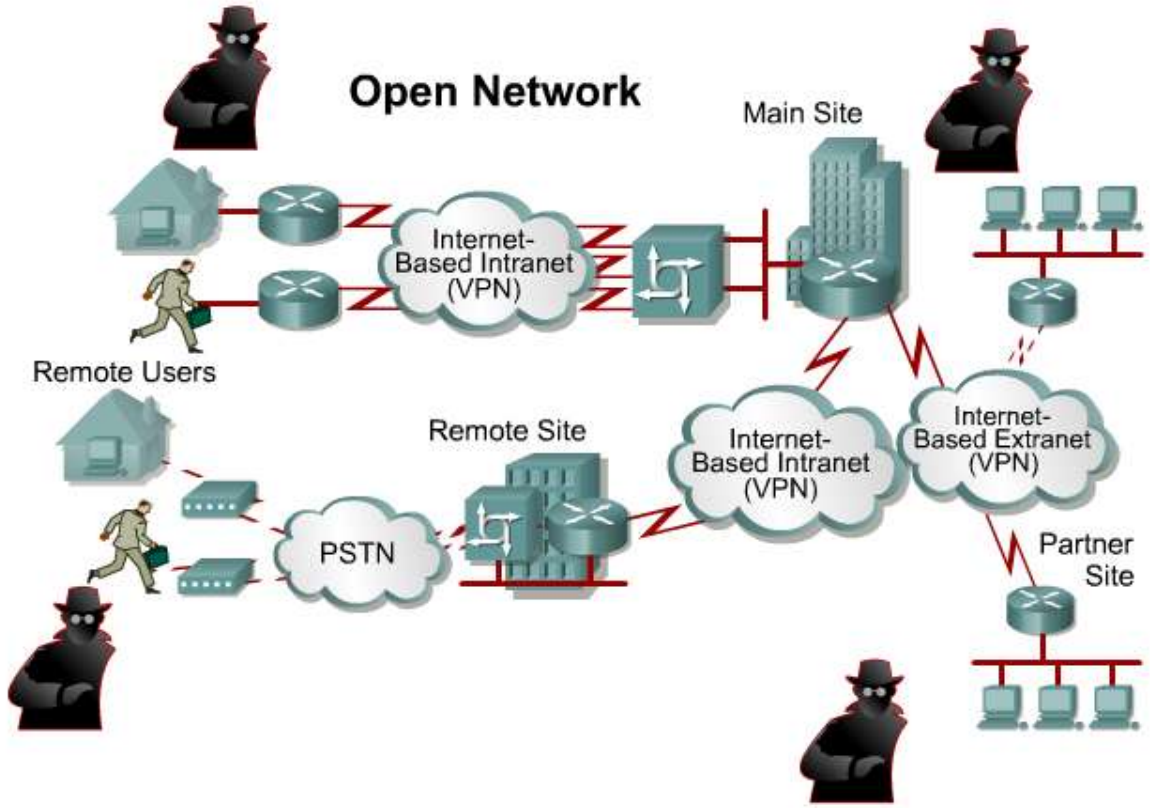
Le but de la sécurité

- Pour protéger les biens!
  - Historiquement réalisé grâce à la sécurité physique et aux réseaux fermés.



Le réseau aujourd'hui

- Avec l'apparition des ordinateurs personnels, les LAN et du monde ouvert avec Internet, les réseaux d'aujourd'hui sont plus ouverts.



Terminologie de la sécurité informatique

» Vulnérabilité

- Une faiblesse qui peut être exploitée par un attaquant dans son avantage, par exemple
  - Environnement physique, bogues logiciels
  - Défauts de conception de protocole / système
  - Mots de passe faibles

» Menace (Threat)

- l'événement ou circonstance qui provoque des dommages aux systèmes, pourrait Exploiter une vulnérabilité, par exemple
  - Physique (incendie, eau, tremblement de terre)
  - Codes malveillants (virus, trojan, logiciels malveillants)
  - Phishing, ingénierie sociale

Terminologie de la sécurité informatique

» Exploit

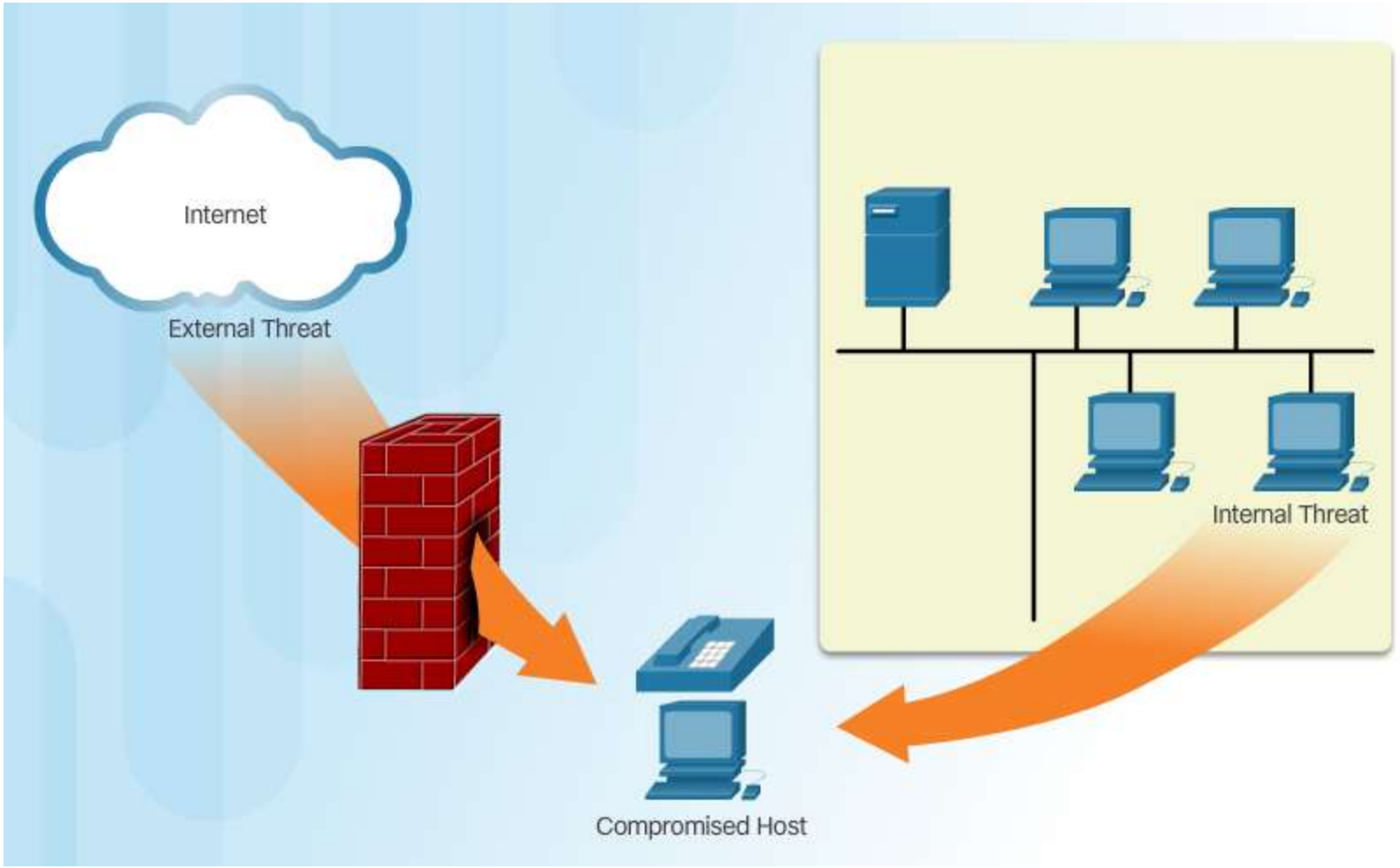
- Mécanisme ou outil utilisé pour tirer parti d'une vulnérabilité, afin de compromettre la sécurité ou la fonctionnalité d'un système
  - Séquence de commandes
  - Pièce de logiciel ou de bloc de données

» Risque

- La probabilité qu'une menace ou un événement se produise
  - Le risque de sécurité ne peut pas être totalement atténué
  - Le risque résiduel est appelé risque résiduel ou risque accepté

إذا كنت تعرف العدو وتعرف نفسك - فلا حاجة بك للخوف من نتائج مئة معركة .. إذا عرفت نفسك لا العدو، فكل نصر تحرزه سيقابله هزيمة تلقاها .. إذا كنت لا تعرف نفسك أو العدو – ستنهزم في كل معركة ..

Vecteurs d'attaques réseau

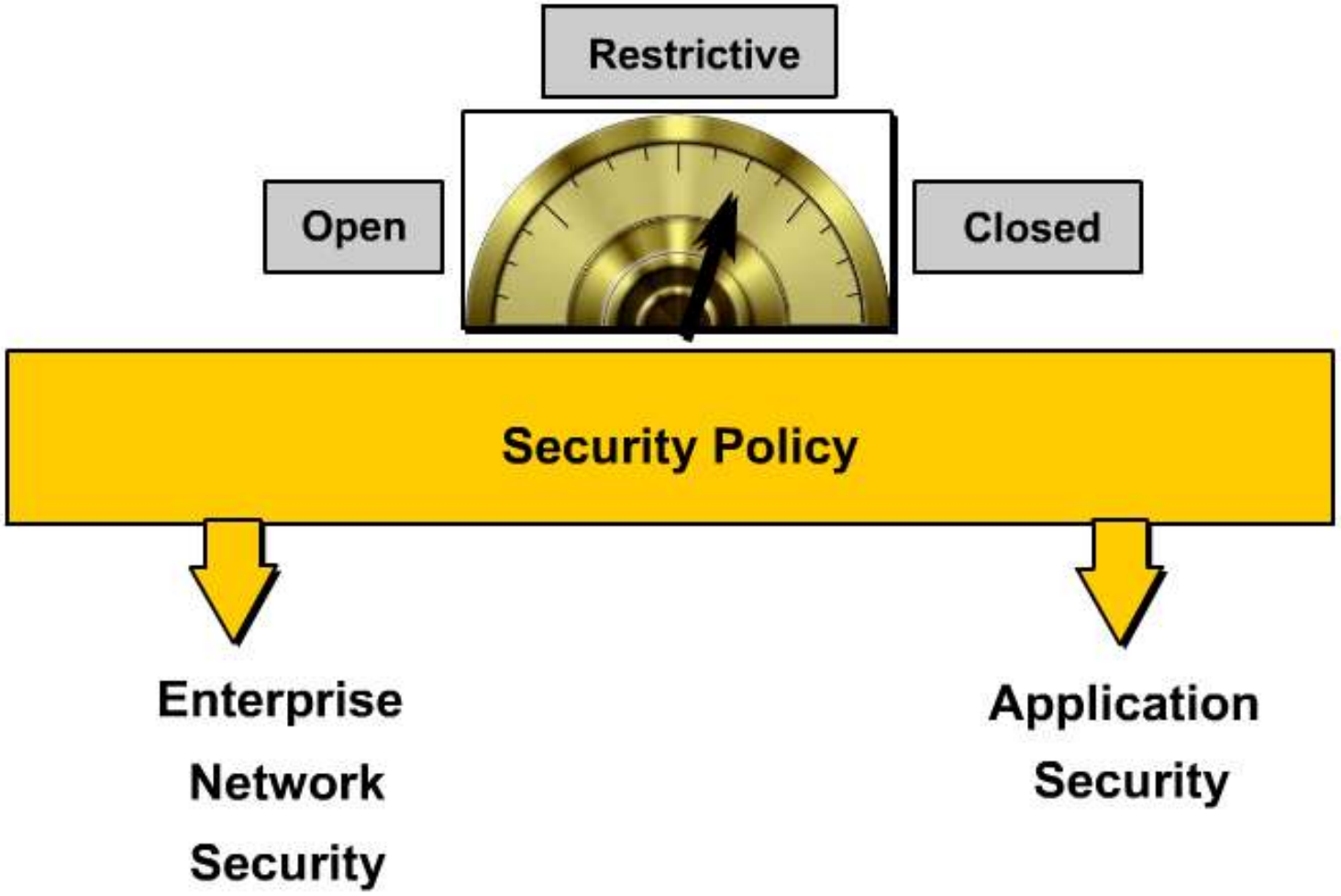


Perte de données

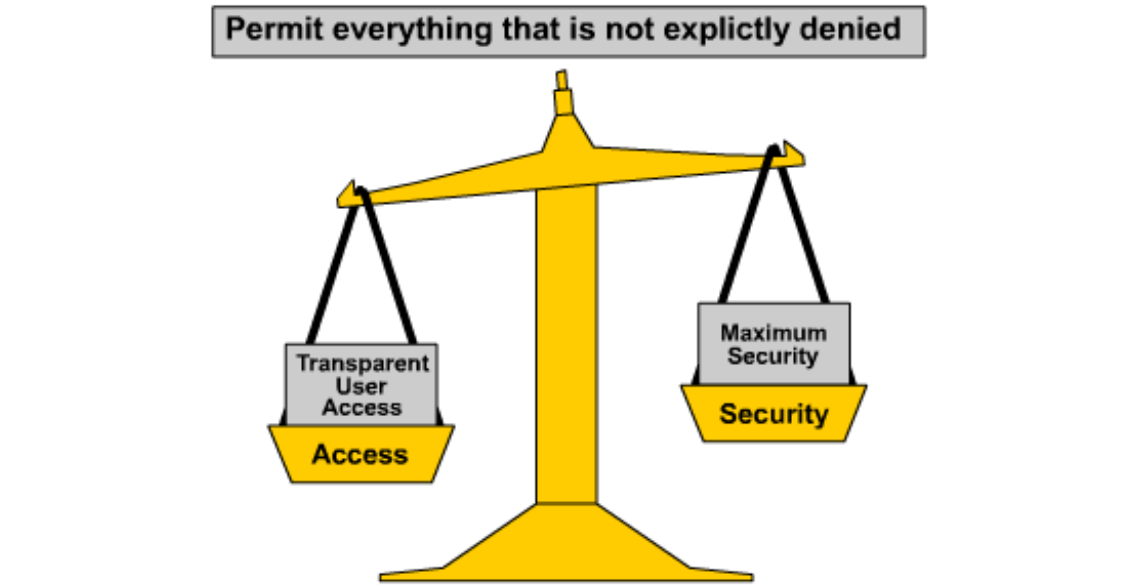
Vecteurs de perte de données:

- Email / Webmail
- Dispositifs non cryptés
- Périphériques de stockage Cloud
- Média amovible
- Copie papier
- Contrôle d'accès incorrect

Modèles de sécurité réseau

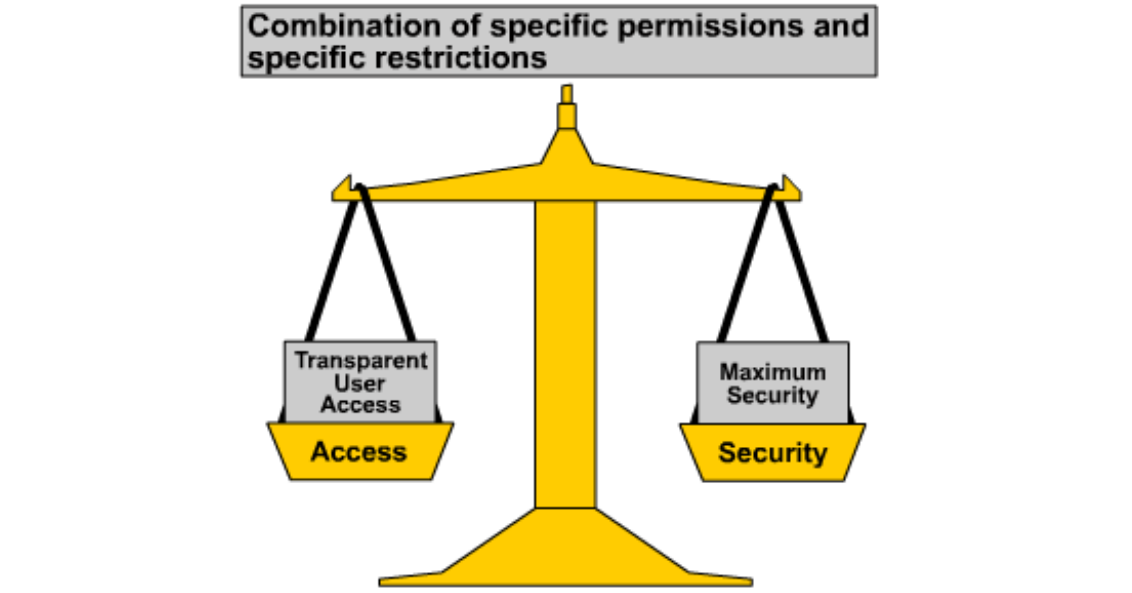


Modèle de sécurité ouvert



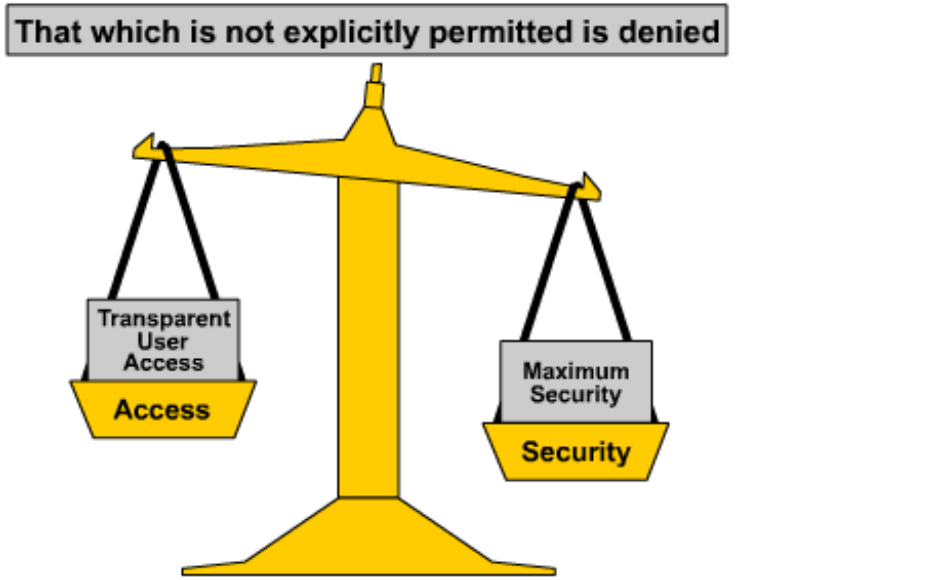
- Facile a configuré et administrer
- Facile pour les utilisateurs réseau
- Cout de sécurité: faible

Modèle de sécurité restreint



- Plus difficile configuré et administrer
- Plus difficile pour les utilisateurs réseau
- Cout de sécurité: élever

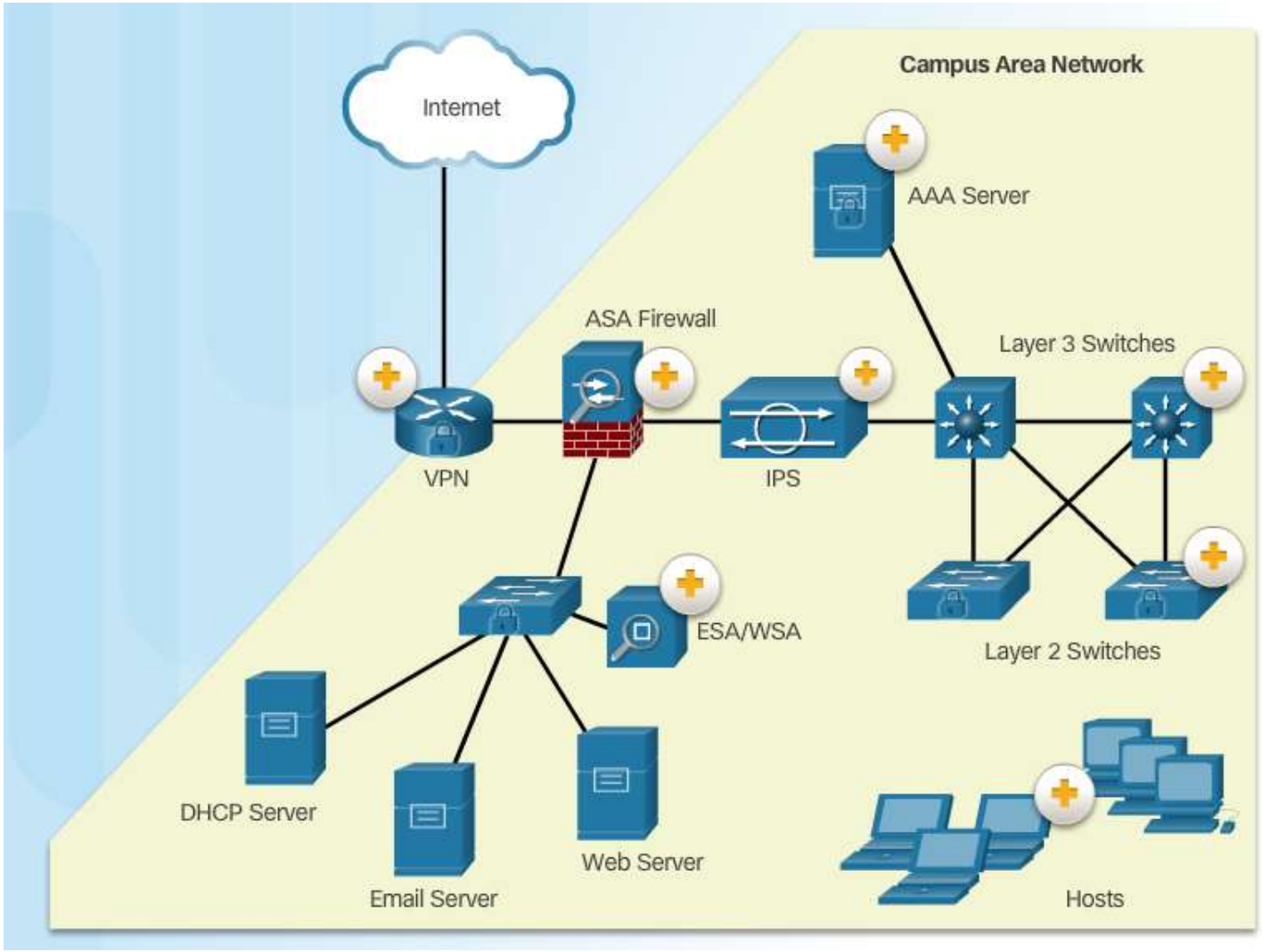
Modèle de sécurité fermé



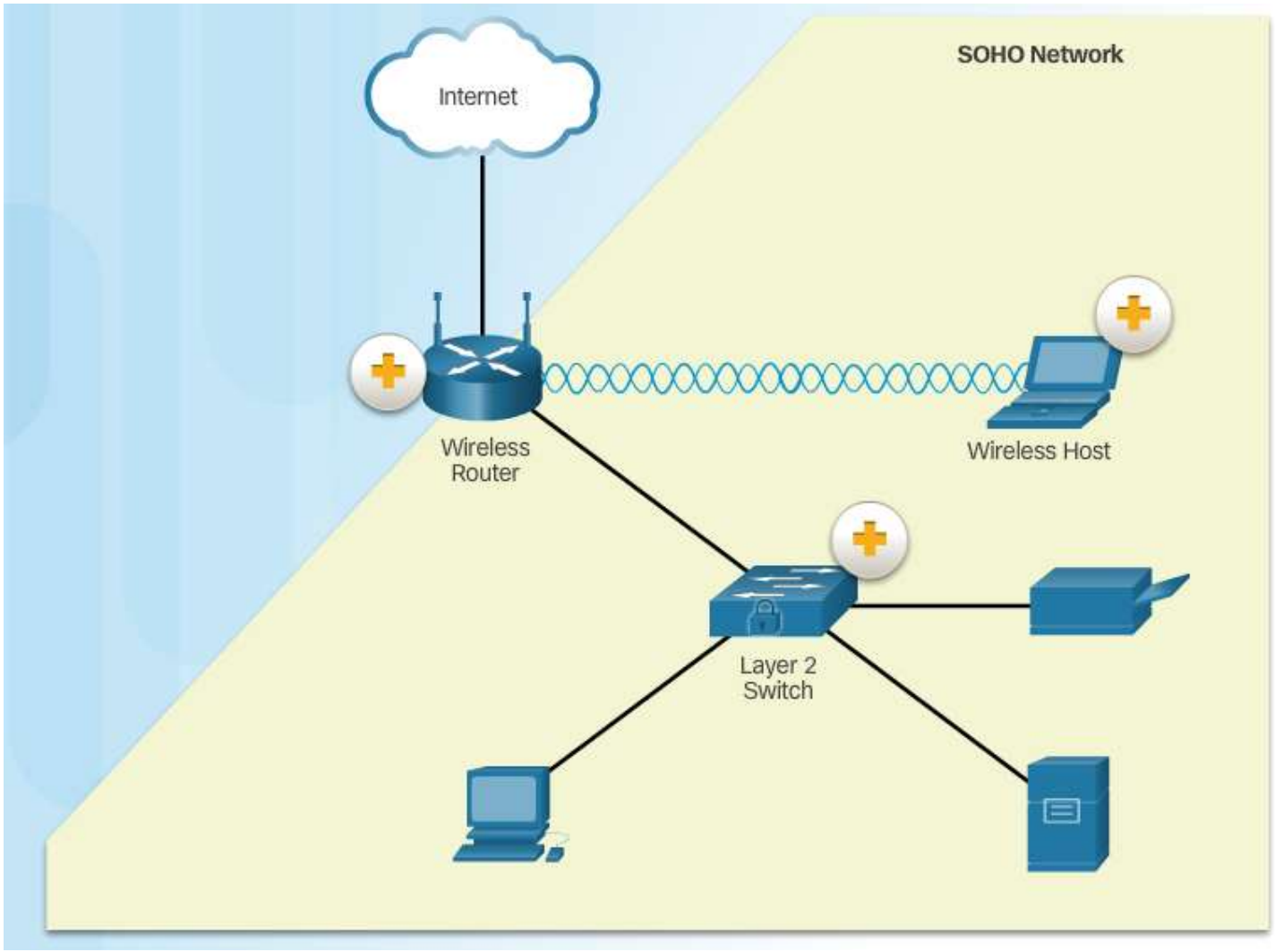
- Plus difficile configuré et administrer
- Plus difficile pour les utilisateurs réseau
- Cout de sécurité: plus élever

1.1.2 Topologie du réseau Vue d'ensemble

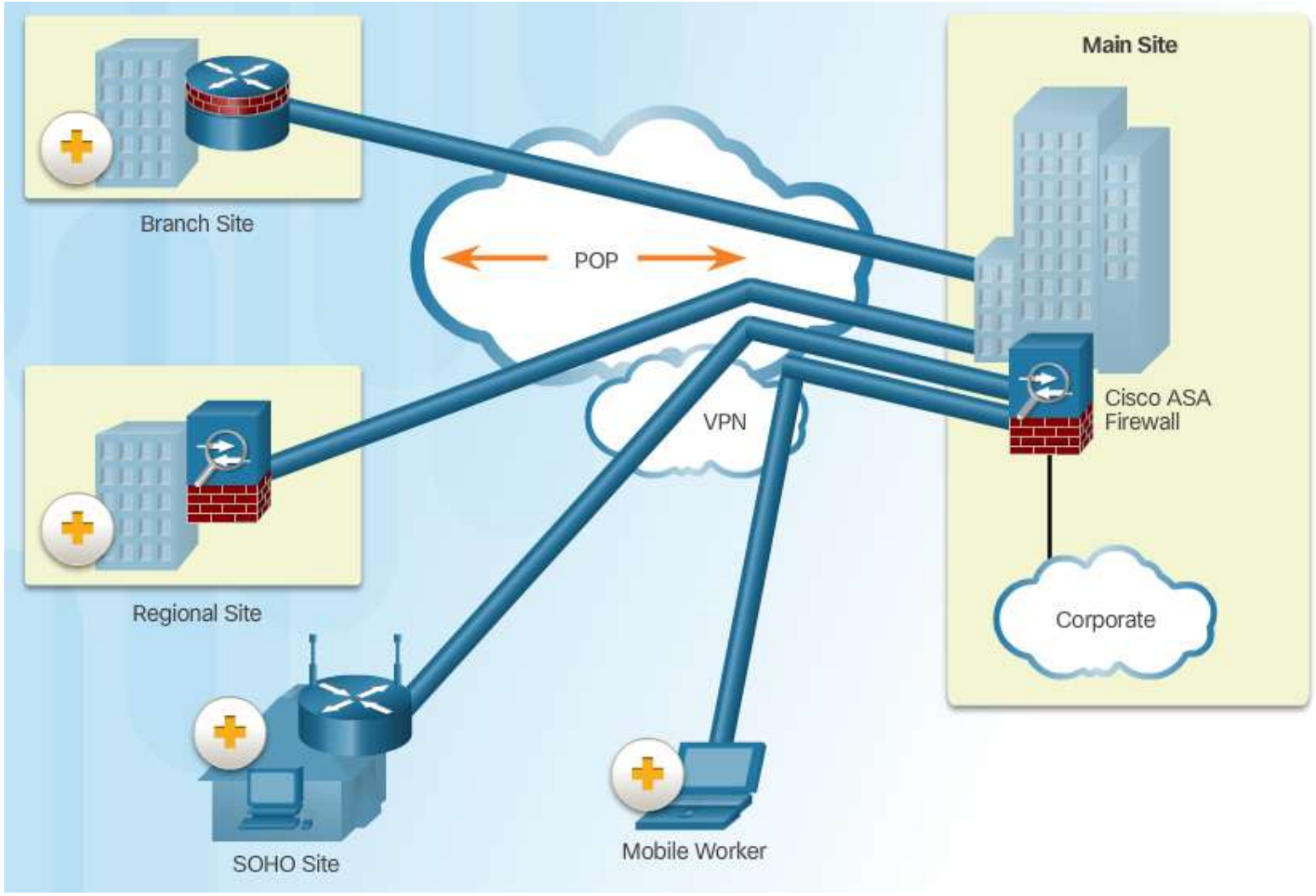
Réseaux de campus



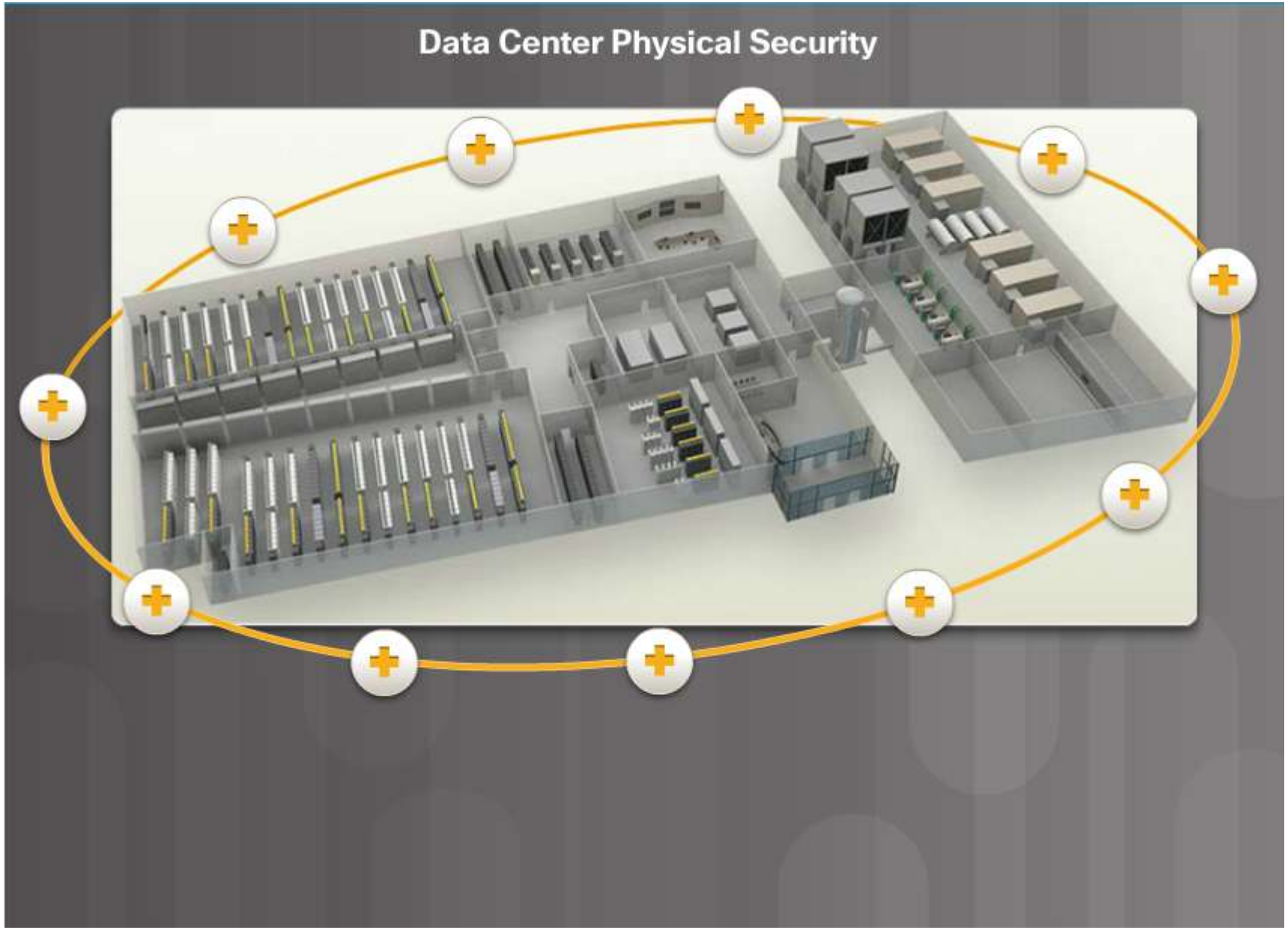
Réseau de Petites et moyennes entreprises



Réseaux étendus (Wide Area Networks)



Data Center Physical Security



Réseaux de centres de données (Data Center)

Sécurité extérieure du périmètre:

- Agents de sécurité sur place
- Clôtures et portails
- Surveillance vidéo continue
- Alarmes de sécurité

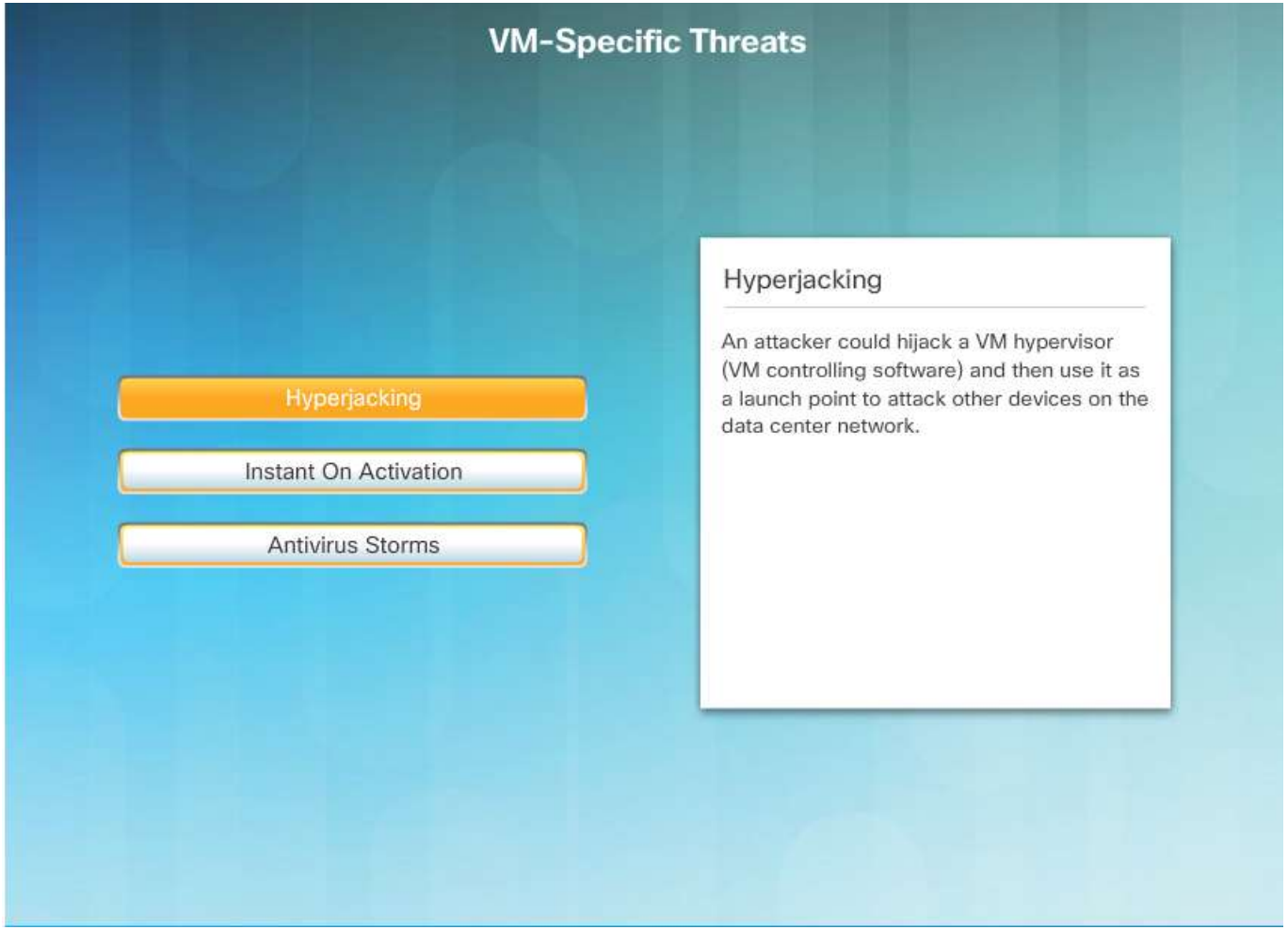
Sécurité à l'intérieur du périmètre:

- Détecteurs de mouvements électroniques
- pièges de sécurité
- Surveillance vidéo continue
- Capteurs biométriques d'accès et de sortie

Cloud et réseaux virtuels

Menaces spécifiques à la VM :

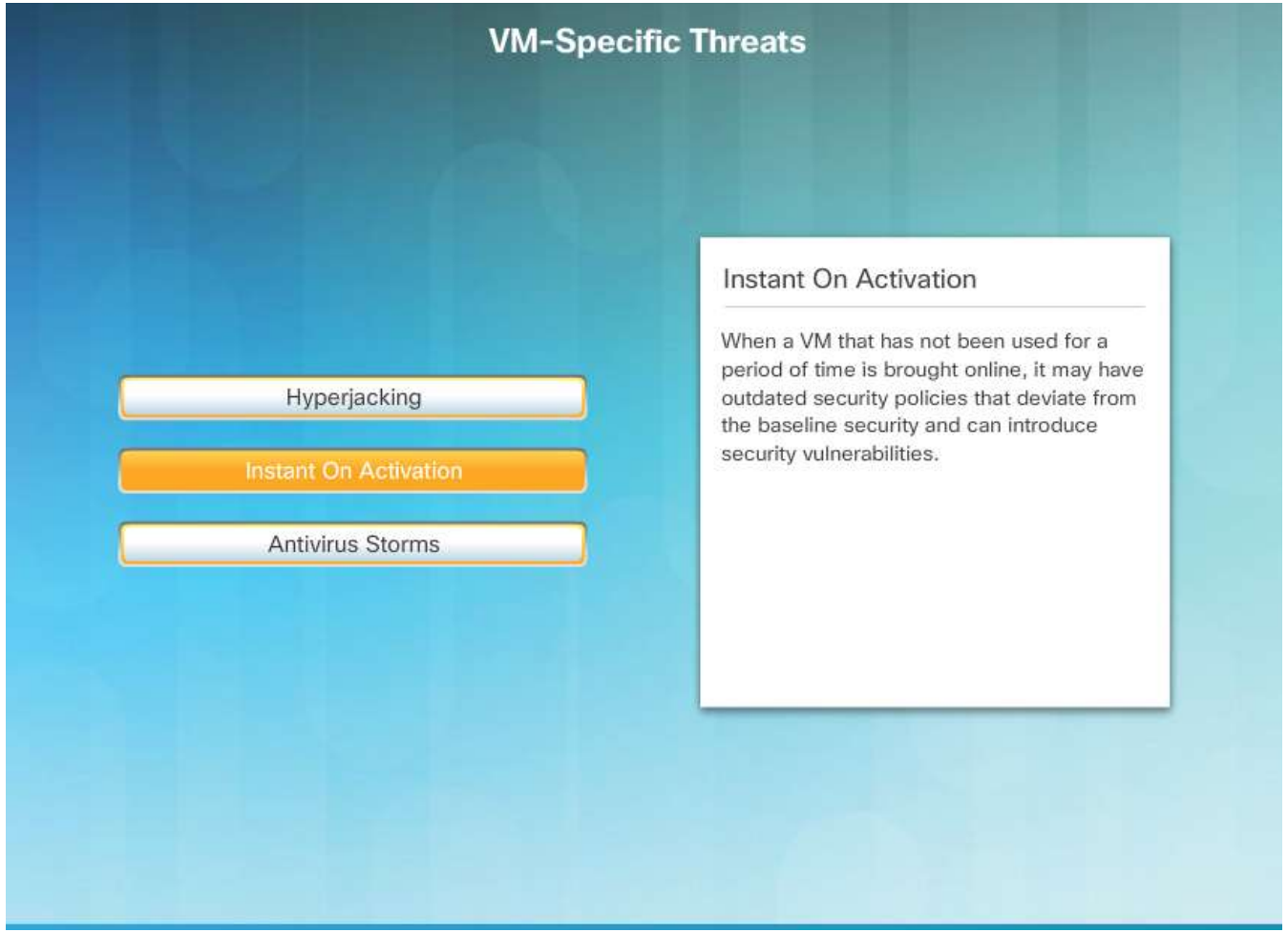
- Hyperjacking
- Instant On activation
- Antivirus storm



Cloud et réseaux virtuels

Menaces spécifiques à la VM :

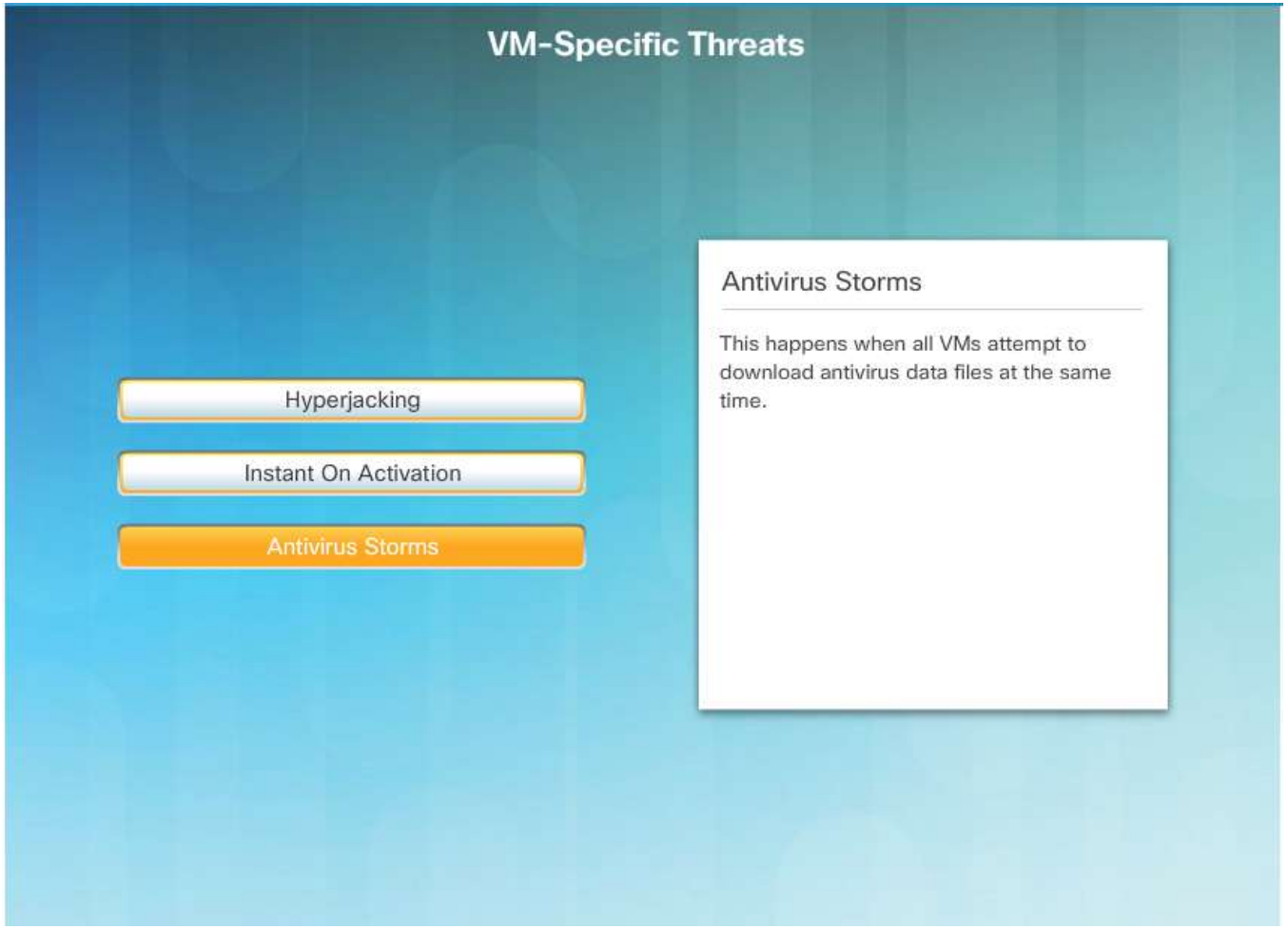
- Hyperjacking
- Instant On activation
- Antivirus storm



Cloud et réseaux virtuels

Menaces spécifiques à la VM :

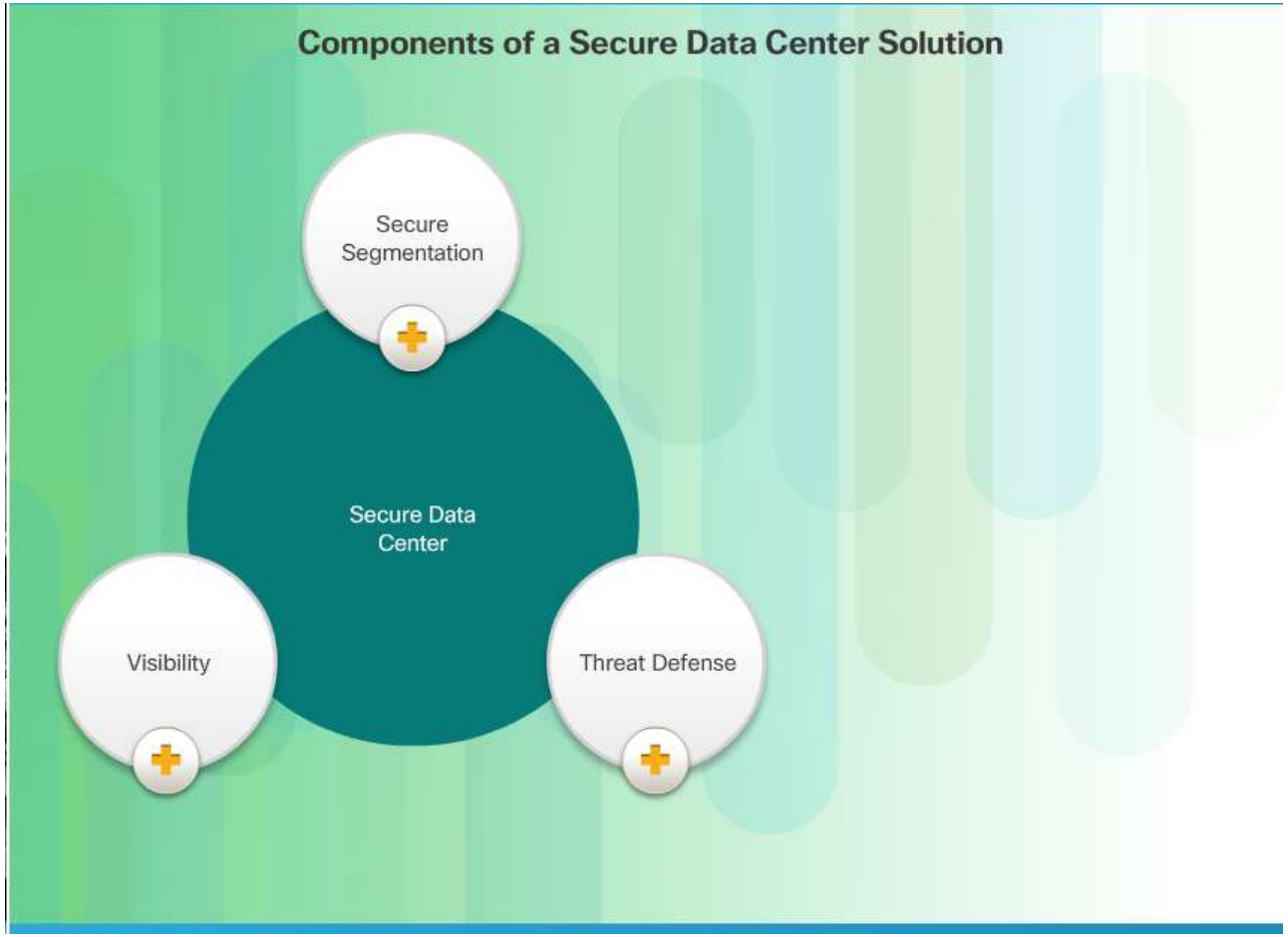
- Hyperjacking
- Instant On activation
- Antivirus storm



Cloud et réseaux virtuels

Composants d'un centre de données sécurisé:

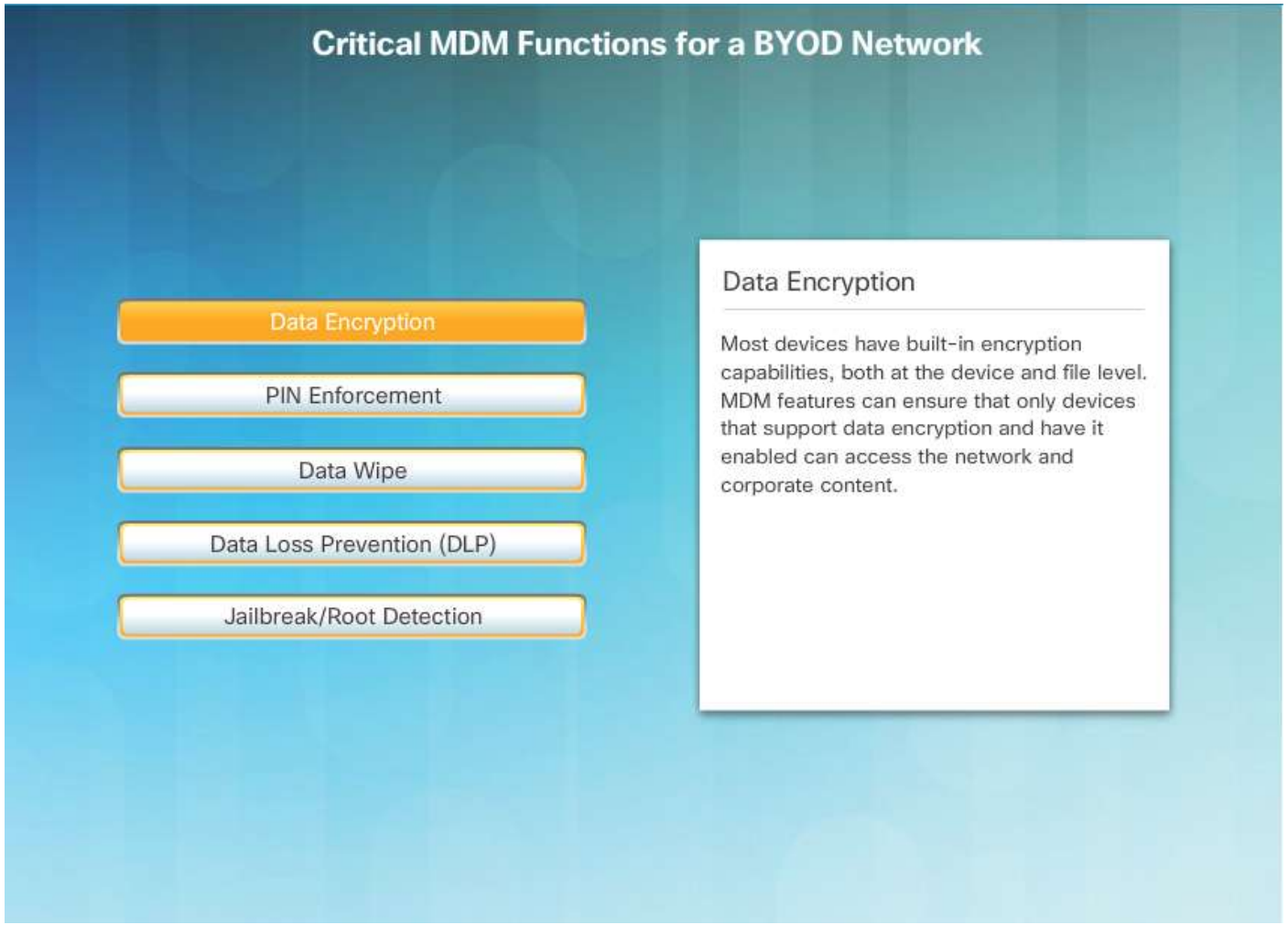
- Segmentation sécurisée
- Défense de la menace
- Visibilité



La frontière du réseau évolutif

Fonctions MDM critiques pour le réseau BYOD:

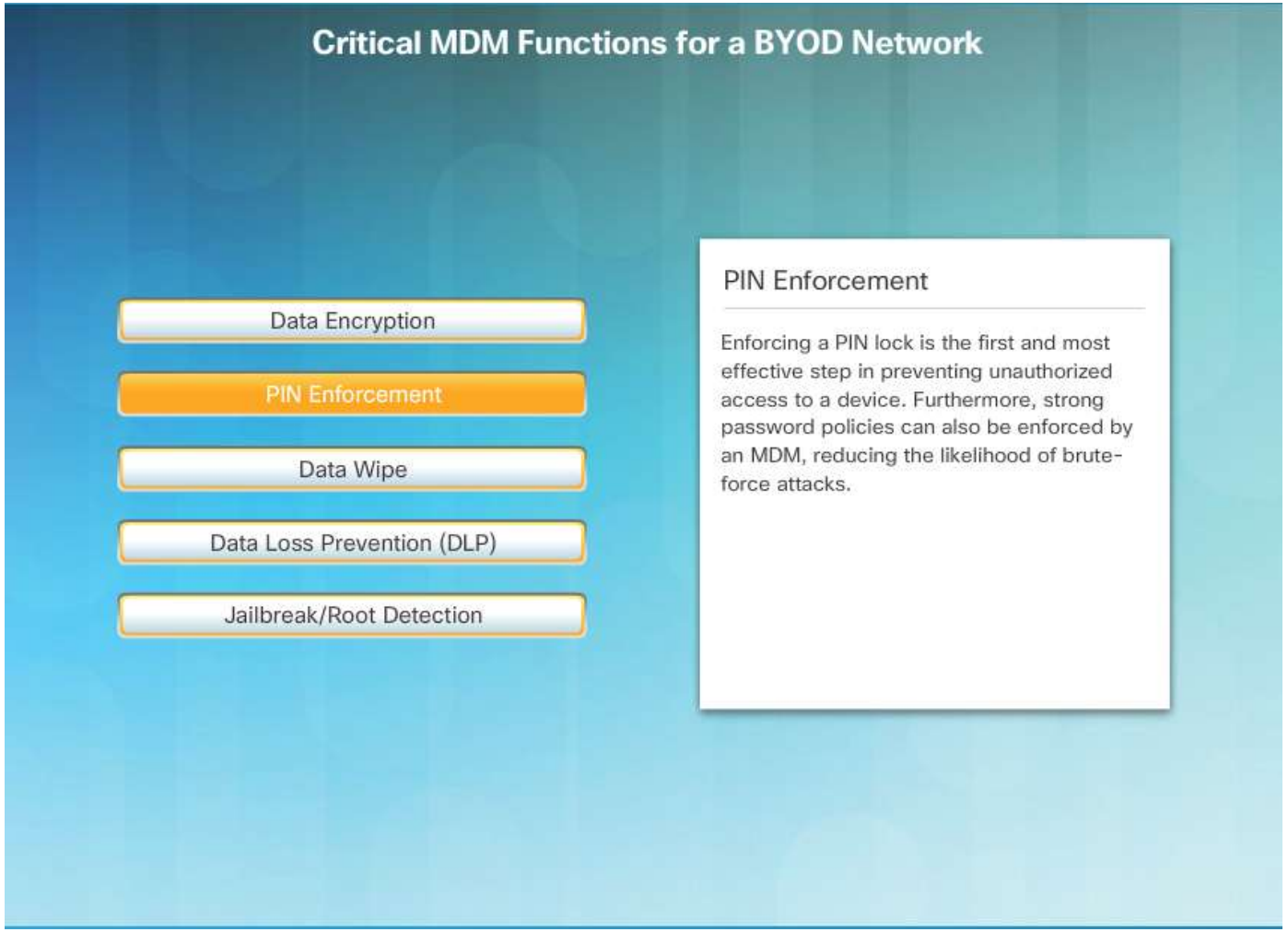
- Cryptage des données



La frontière du réseau évolutif

Fonctions MDM critiques pour le réseau BYOD:

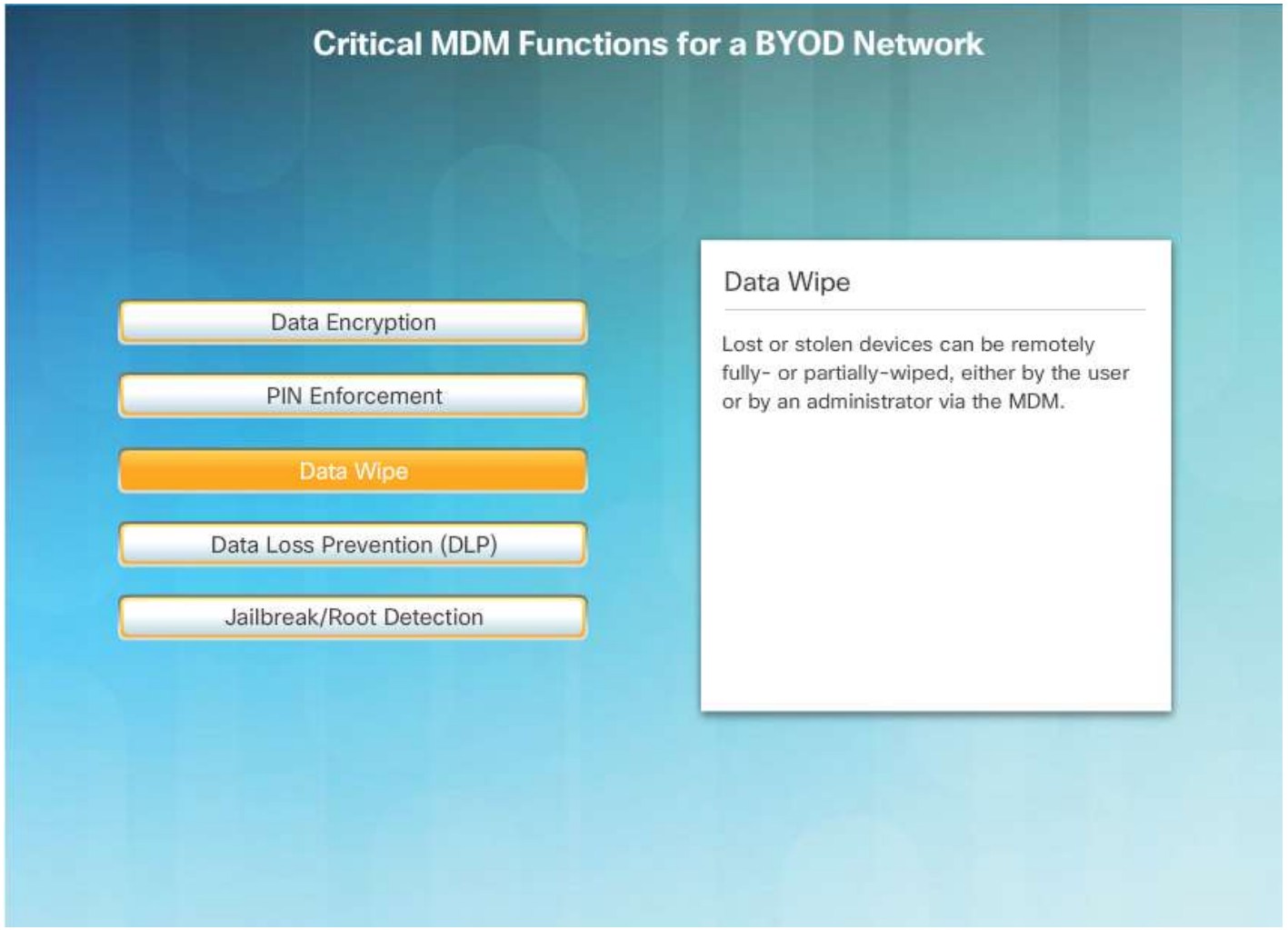
- Forcement de PIN



La frontière du réseau évolutif

Fonctions MDM critiques pour le réseau BYOD:

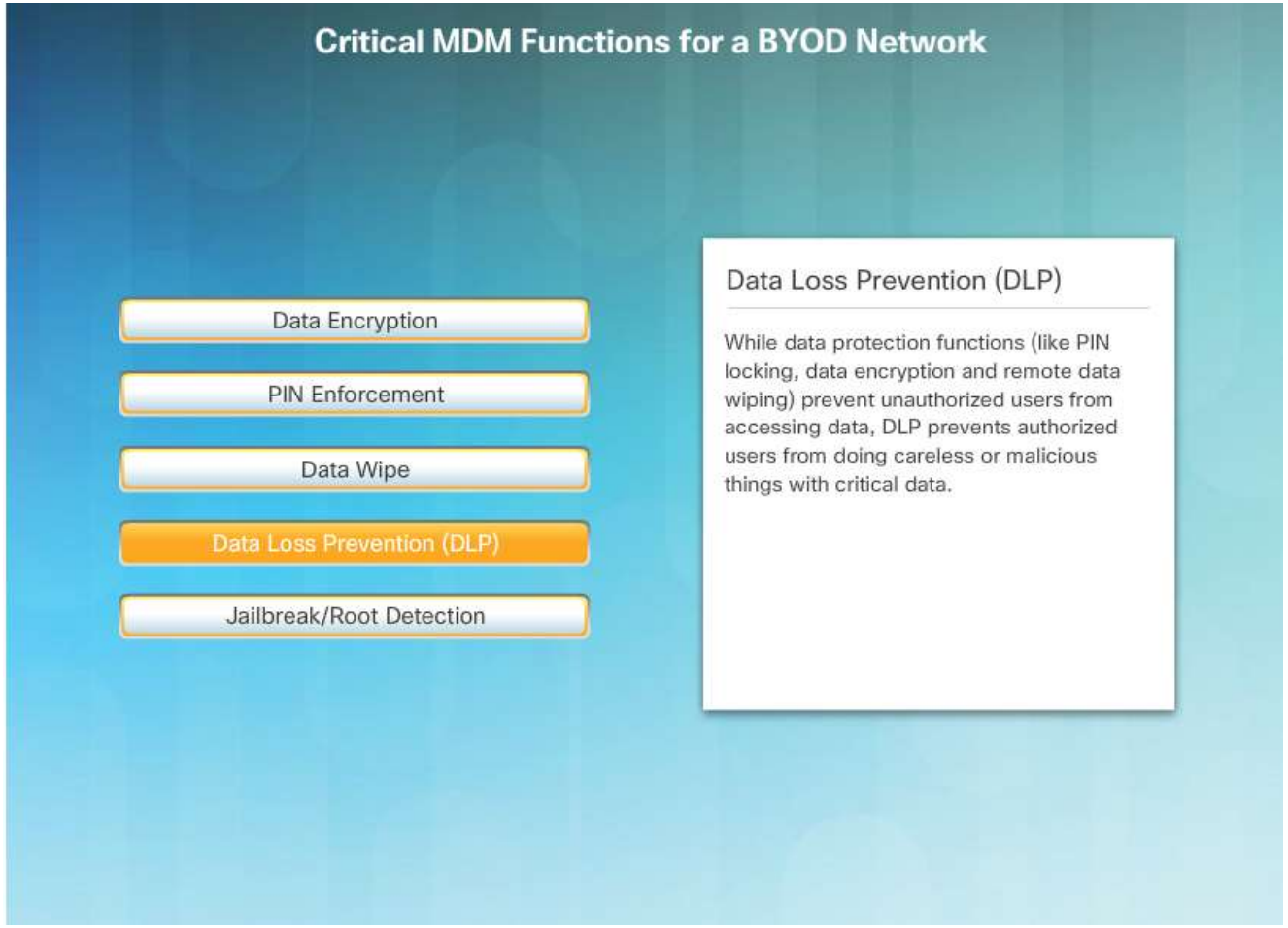
- éffacer les données



La frontière du réseau évolutif

Fonctions MDM critiques pour le réseau BYOD:

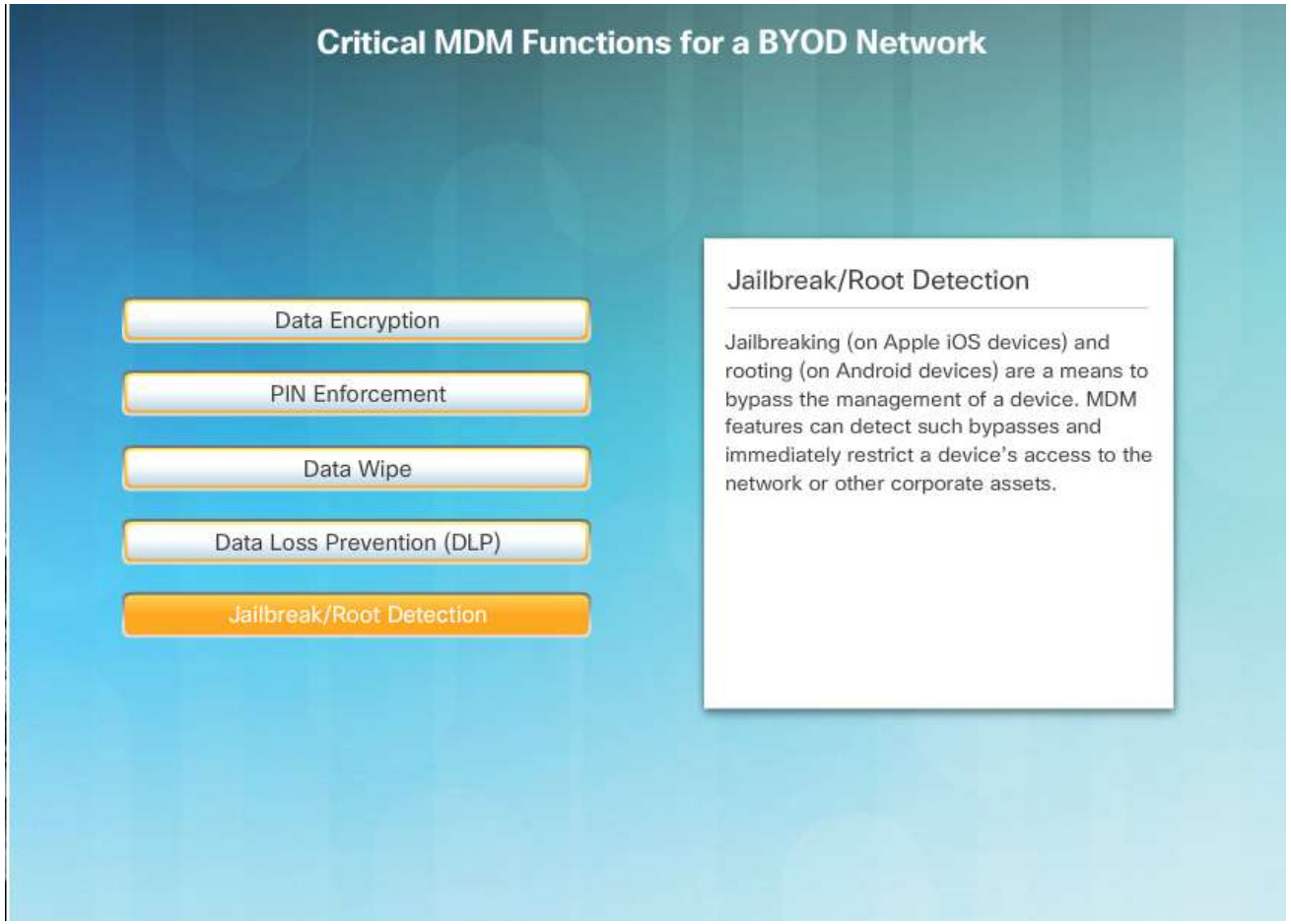
- Prévoir les pertes de données



La frontière du réseau évolutif

Fonctions MDM critiques pour le réseau BYOD:

- Jailbreak/root detection



Section 1.2: Menaces réseau

À la fin de la section, vous devriez pouvoir:

- Décrire l'évolution de la sécurité des réseaux.
- Décrire les différents types d'outils d'attaque utilisés par les pirates informatiques.
- Décrire les logiciels malveillants.
- Expliquez les courantes attaques réseau.

1.2.1 Qui est entrain de pirater (Hacker) Nos Réseaux?

Le Hacker et l'évolution des pirates

Les pirates moderne:

- Script Kiddies
- Vulnerability Brokers
- Hacktivists
- Cyber Criminals
- State-Sponsored Hackers

Le Hacker et l'évolution des pirates

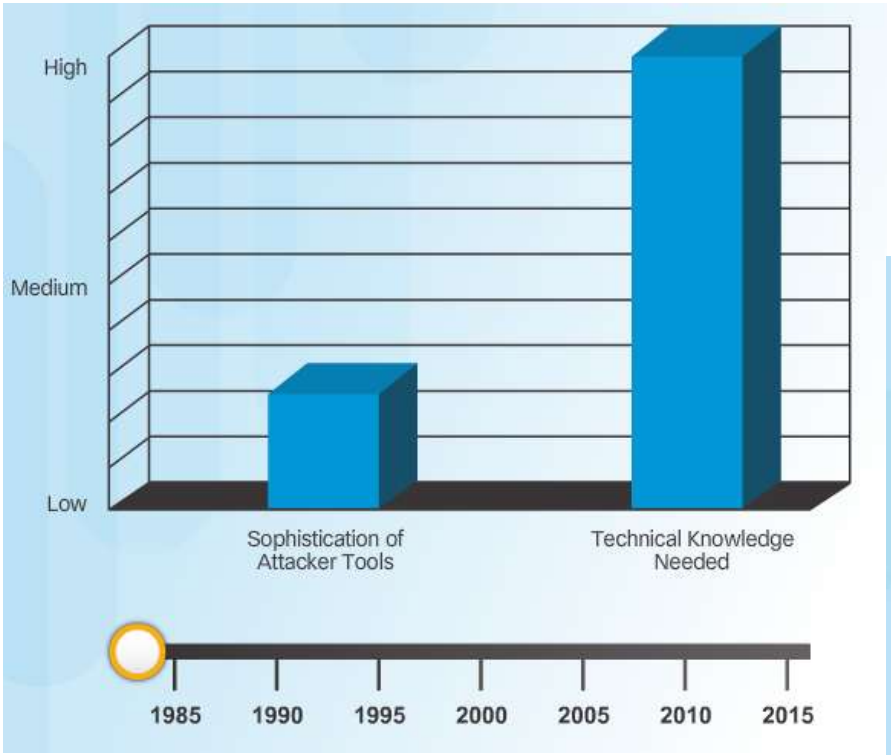
Cyber Criminals

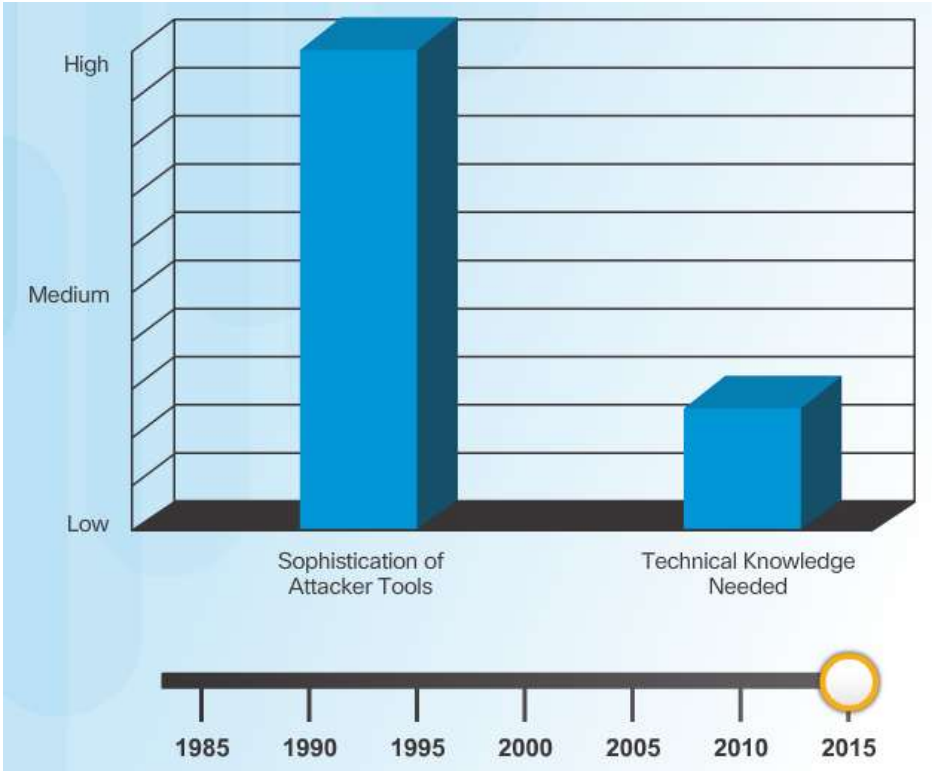
Anonymous Hacktivist Group

State-Sponsored Hackers

1.2.2 Les outils des Hackers

Introduction sur les outils d'attaque





Evolution des outils de sécurité

Outils de test de pénétration:

- Craqueur de Mot de passe
- Le piratage sans fil
- Scanneur réseau et piratage
- Fabrication de paquets
- Renifleurs de paquets
- Détecteurs de rootkits
- Fuzzers (test aléatoire) pour rechercher des vulnérabilités

- Légal (Forensic)
- Débogueurs
- Hacking des systèmes d'exploitation
- Chiffrement
- Exploitation de la vulnérabilité
- Scanners de vulnérabilité

Penetration Testing Tools

- Password Crackers
- Wireless Hacking Tools
- Network Scanning and Hacking Tools
- Packet Crafting Tools
- Packet Sniffers
- Rootkit Detectors
- Fuzzers to Search Vulnerabilities

Password Crackers

Passwords are the most vulnerable security threat. Password cracking tools are often referred to as password recovery tools and can be used to crack or recover the password. This is accomplished either by removing the original password, after bypassing the data encryption, or by outright discovery of the password. Password crackers repeatedly make guesses in order to crack the password and access the system. Examples of password cracking tools include John the Ripper, Ophcrack, L0phtCrack, THC Hydra, RainbowCrack, and Medusa.

Penetration Testing Tools

- Password Crackers
- Wireless Hacking Tools
- Network Scanning and Hacking Tools
- Packet Crafting Tools
- Packet Sniffers
- Rootkit Detectors
- Fuzzers to Search Vulnerabilities

Wireless Hacking Tools

Wireless networks are more susceptible to network security threats. Wireless hacking tools are used to intentionally hack into a wireless network to detect security vulnerabilities. Examples of wireless hacking tools include Aircrack-ng, Kismet, InSSIDer, KisMAC, Firesheep, and NetStumbler.

Penetration Testing Tools

- Password Crackers
- Wireless Hacking Tools
- Network Scanning and Hacking Tools
- Packet Crafting Tools
- Packet Sniffers
- Rootkit Detectors
- Fuzzers to Search Vulnerabilities

Network Scanning and Hacking Tools

Network scanning tools are used to probe network devices, servers, and hosts for open TCP or UDP ports. Examples of scanning tools include Nmap, SuperScan, Angry IP Scanner, and NetScanTools.

Penetration Testing Tools

- Password Crackers
- Wireless Hacking Tools
- Network Scanning and Hacking Tools
- Packet Crafting Tools
- Packet Sniffers
- Rootkit Detectors
- Fuzzers to Search Vulnerabilities

Packet Crafting Tools

These tools are used to probe and test a firewall's robustness using specially crafted forged packets. Examples of such tools include Hping, Scapy, Socat, Yersinia, Netcat, Nping, and Nemesis.

Penetration Testing Tools

- Password Crackers
- Wireless Hacking Tools
- Network Scanning and Hacking Tools
- Packet Crafting Tools
- Packet Sniffers
- Rootkit Detectors
- Fuzzers to Search Vulnerabilities

Packet Sniffers

These tools are used to capture and analyze packets within traditional Ethernet LANs or WLANs. Tools include Wireshark, Tcpdump, Ettercap, Dsniff, EtherApe, Paros, Fiddler, Ratproxy, and SSLstrip.

Penetration Testing Tools

- Password Crackers
- Wireless Hacking Tools
- Network Scanning and Hacking Tools
- Packet Crafting Tools
- Packet Sniffers
- Rootkit Detectors
- Fuzzers to Search Vulnerabilities

Rootkit Detectors

This is a directory and file integrity checker used by white hats to detect installed root kits. Example tools include AIDE, Netfilter, and PF: OpenBSD Packet Filter.

Penetration Testing Tools

- Password Crackers
- Wireless Hacking Tools
- Network Scanning and Hacking Tools
- Packet Crafting Tools
- Packet Sniffers
- Rootkit Detectors
- Fuzzers to Search Vulnerabilities

Fuzzers to Search Vulnerabilities

Fuzzers are tools used by hackers when attempting to discover a computer system's security vulnerabilities. Examples of fuzzers include Skipfish, Wapiti, and W3af.

Penetration Testing Tools (Cont.)

- Forensic Tools
- Debuggers
- Hacking Operating Systems
- Encryption Tools
- Vulnerability Exploitation Tools
- Vulnerability Scanners

Forensic Tools

These tools are used by white hat hackers to sniff out any trace of evidence existing in a particular computer system. Example of tools include Sleuth Kit, Helix, Maltego, and Encase.

Penetration Testing Tools (Cont.)

- Forensic Tools
- Debuggers
- Hacking Operating Systems
- Encryption Tools
- Vulnerability Exploitation Tools
- Vulnerability Scanners

Debuggers

These tools are used by black hats to reverse engineer binary files when writing exploits. They are also used by white hats when analyzing malware. Debugging tools include GDB, WinDbg, IDA Pro, and Immunity Debugger.

Penetration Testing Tools (Cont.)

- Forensic Tools
- Debuggers
- Hacking Operating Systems
- Encryption Tools
- Vulnerability Exploitation Tools
- Vulnerability Scanners

Hacking Operating Systems

These are specially designed operating systems preloaded with tools and technologies optimized for hacking. Examples of specially designed hacking operating systems include Kali Linux, SELinux, Knoppix, BackBox Linux.

Penetration Testing Tools (Cont.)

- Forensic Tools
- Debuggers
- Hacking Operating Systems
- Encryption Tools
- Vulnerability Exploitation Tools
- Vulnerability Scanners

Encryption Tools

These tools safeguard the contents of an organization's data at rest and data in motion. Encryption tools use algorithm schemes to encode the data to prevent unauthorized access to the encrypted data. Examples of these tools include VeraCrypt, CipherShed, OpenSHH, OpenSSL, Tor, OpenVPN, and Stunnel.

Penetration Testing Tools (Cont.)

- Forensic Tools
- Debuggers
- Hacking Operating Systems
- Encryption Tools
- Vulnerability Exploitation Tools
- Vulnerability Scanners

Vulnerability Exploitation Tools

These tools identify whether a remote host is vulnerable to a security attack. Examples of vulnerability exploitation tools include Metasploit, Core Impact, Sqlmap, Social Engineer Toolkit, and Netsparker.

Penetration Testing Tools (Cont.)

- Forensic Tools
- Debuggers
- Hacking Operating Systems
- Encryption Tools
- Vulnerability Exploitation Tools
- Vulnerability Scanners

Vulnerability Scanners

These tools scan a network or system to identify open ports. They can also be used to scan for known vulnerabilities and scan VMs, BYOD devices, and client databases. Examples of tools include Nipper, Secunia PSI, Core Impact, Nessus v6, SAINT, and Open VAS.

Catégories d'outils d'attaque

Attaques de piratage réseau:

- Eavesdropping
- Modification des données
- Spoofing d'adresses IP
- Basé sur le Mot de passe
- Déni de service
- L'homme au milieu
- Clé compromise
- Sniffer

Network Hacking Attacks

- Eavesdropping Attack
- Data Modification Attack
- IP Address Spoofing Attack
- Password-Based Attacks
- Denial-of-Service Attack
- Man-in-the-Middle Attack
- Compromised-Key Attack
- Sniffer Attack

Eavesdropping Attack

This is when a hacker captures and "listens" to network traffic. This attack is also referred to as sniffing or snooping.

Network Hacking Attacks

- Eavesdropping Attack
- Data Modification Attack
- IP Address Spoofing Attack
- Password-Based Attacks
- Denial-of-Service Attack
- Man-in-the-Middle Attack
- Compromised-Key Attack
- Sniffer Attack

Data Modification Attack

If hackers have captured enterprise traffic, they can alter the data in the packet without the knowledge of the sender or receiver.

Network Hacking Attacks

- Eavesdropping Attack
- Data Modification Attack
- IP Address Spoofing Attack
- Password-Based Attacks
- Denial-of-Service Attack
- Man-in-the-Middle Attack
- Compromised-Key Attack
- Sniffer Attack

IP Address Spoofing Attack

A hacker constructs an IP packet that appears to originate from a valid address inside the corporate intranet.

Network Hacking Attacks

- Eavesdropping Attack
- Data Modification Attack
- IP Address Spoofing Attack
- Password-Based Attacks
- Denial-of-Service Attack
- Man-in-the-Middle Attack
- Compromised-Key Attack
- Sniffer Attack

Password-Based Attacks

If hackers discover a valid user account, the attackers have the same rights as the real user. Hackers could use that valid account to obtain lists of other users and network information. They could also change server and network configurations, modify, reroute, or delete data.

Network Hacking Attacks

- Eavesdropping Attack
- Data Modification Attack
- IP Address Spoofing Attack
- Password-Based Attacks
- Denial-of-Service Attack
- Man-in-the-Middle Attack
- Compromised-Key Attack
- Sniffer Attack

Denial-of-Service Attack

A DoS attack prevents normal use of a computer or network by valid users. After gaining access to your network, a DoS attack can crash applications or network services. A DoS attack can also flood a computer or the entire network with traffic until a shutdown occurs because of the overload. A DoS attack can also block traffic, which results in a loss of access to network resources by authorized users.

Network Hacking Attacks

- Eavesdropping Attack
- Data Modification Attack
- IP Address Spoofing Attack
- Password-Based Attacks
- Denial-of-Service Attack
- Man-in-the-Middle Attack
- Compromised-Key Attack
- Sniffer Attack

Man-in-the-Middle Attack

This attack occurs when hackers have positioned themselves between a source and destination. They can now actively monitor, capture, and control the communication transparently.

Network Hacking Attacks

- Eavesdropping Attack
- Data Modification Attack
- IP Address Spoofing Attack
- Password-Based Attacks
- Denial-of-Service Attack
- Man-in-the-Middle Attack
- Compromised-Key Attack
- Sniffer Attack

Compromised-Key Attack

If a hacker obtains a secret key, that key is referred to as a compromised key. A compromised key can be used to gain access to a secured communication without the sender or receiver being aware of the attack.

Network Hacking Attacks

- Eavesdropping Attack
- Data Modification Attack
- IP Address Spoofing Attack
- Password-Based Attacks
- Denial-of-Service Attack
- Man-in-the-Middle Attack
- Compromised-Key Attack
- Sniffer Attack

Sniffer Attack

A sniffer is an application or device that can read, monitor, and capture network data exchanges and read network packets. If the packets are not encrypted, a sniffer provides a full view of the data inside the packet. Even encapsulated (tunneled) packets can be broken open and read unless they are encrypted and the attacker does not have access to the key.

1.2.3 Malware


messages
virus
address
advertising
technology
sent
access
spammers
forged
fraud
information
worm
unsuccessful
damage
attack
malware
illegal
media
junk
mailing
abuse
against
service
legislation
public

Malware

- “Malicious software” Est un logiciel conçu pour infiltrer un ordinateur sans la volonté du propriétaire.
- Malware inclus:
  - Des virus informatiques
  - Vers
  - chevaux de Troie
  - rootkits
  - Backdoors (Méthode de contournement des procédures d'authentification normales et généralement installée à l'aide de chevaux de Troie ou de vers.)
  - Pour le profit (Spyware, botnets, keyloggers et dialers)

Pourquoi écrire un code malveillant?

- La plupart des premiers vers et des virus ont été écrits comme des expériences ou des farces généralement conçus pour être inoffensifs ou simplement ennuyeux plutôt que de causer des dommages sérieux aux ordinateurs.
- Les jeunes programmeurs apprenant sur les virus et les techniques les ont écrits dans le seul but qu'ils pouvaient ou pour voir jusqu'à quel point il pourrait se propager.
- Dans certains cas, l'auteur n'a pas réalisé combien de dommages leurs créations pouvaient faire.
- Jusqu'en 1999, les virus répandus tels que le virus Melissa semblent avoir été écrits principalement comme des farces.

Écriture de code malveillante aujourd'hui

L'écriture de codes malveillants a changé pour des raisons rentables.

- Principalement en raison de l'Internet et l'accès à large bande.
- Depuis 2003, la majorité des virus et des vers ont été conçus pour prendre le contrôle des ordinateurs des utilisateurs pour l'exploitation du marché noir.
- Les «ordinateurs zombies» infectés sont utilisés pour envoyer du courrier électronique, pour héberger des données de contrebande ou pour attaquer DDoS comme une forme d'extorsion.

En 2008, Symantec a publié:

- Le taux de libération du code malveillant et d'autres programmes indésirables peut être supérieur à celui des applications logicielles légitimes.

Virus, chevaux de Troie et vers

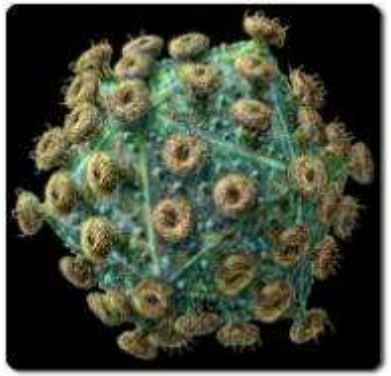
- Un **virus** est un logiciel malveillant qui est attaché à un autre programme pour exécuter une fonction indésirable particulière sur la station de travail d'un utilisateur.
- Un **ver** exécute du code arbitraire et installe des copies de lui-même dans la mémoire de l'ordinateur infecté, qui infecte les autres hôtes.
- Un **cheval de Troie** n'est différent que parce que l'application entière a été écrite pour ressembler à autre chose, alors qu'en fait c'est un outil d'attaque.

Viruses


Virus Alert!
Warning! Threat detected!
A malicious item has been detected!

Viruses

- ✓ Un virus informatique est un programme informatique malveillant (fichier exécutable) qui peut se copier et infecter un ordinateur sans autorisation ni connaissance de l'utilisateur.
- ✓ Un virus ne peut se propager d'un ordinateur à un autre que par:
  - ❑ L'envoi sur un réseau en tant que fichier ou en tant que charge utile d'email.
  - ❑ Le transporter sur un support amovible.
- ✓ Les virus ont besoin de l'INTERVENTION ...



Cheval de Troie

- Un cheval de Troie est un programme qui apparaît, à l'utilisateur, pour effectuer une fonction souhaitable, mais qui, en fait, facilite l'accès non autorisé au système informatique de l'utilisateur.
- Les chevaux de Troie peuvent sembler être des programmes utiles ou intéressants, ou tout au moins inoffensifs pour un utilisateur non méfiant.
- Les chevaux de Troie ne se reproduisent pas eux-mêmes, ce qui les distingue des virus et des vers.

Classement du cheval de Troie

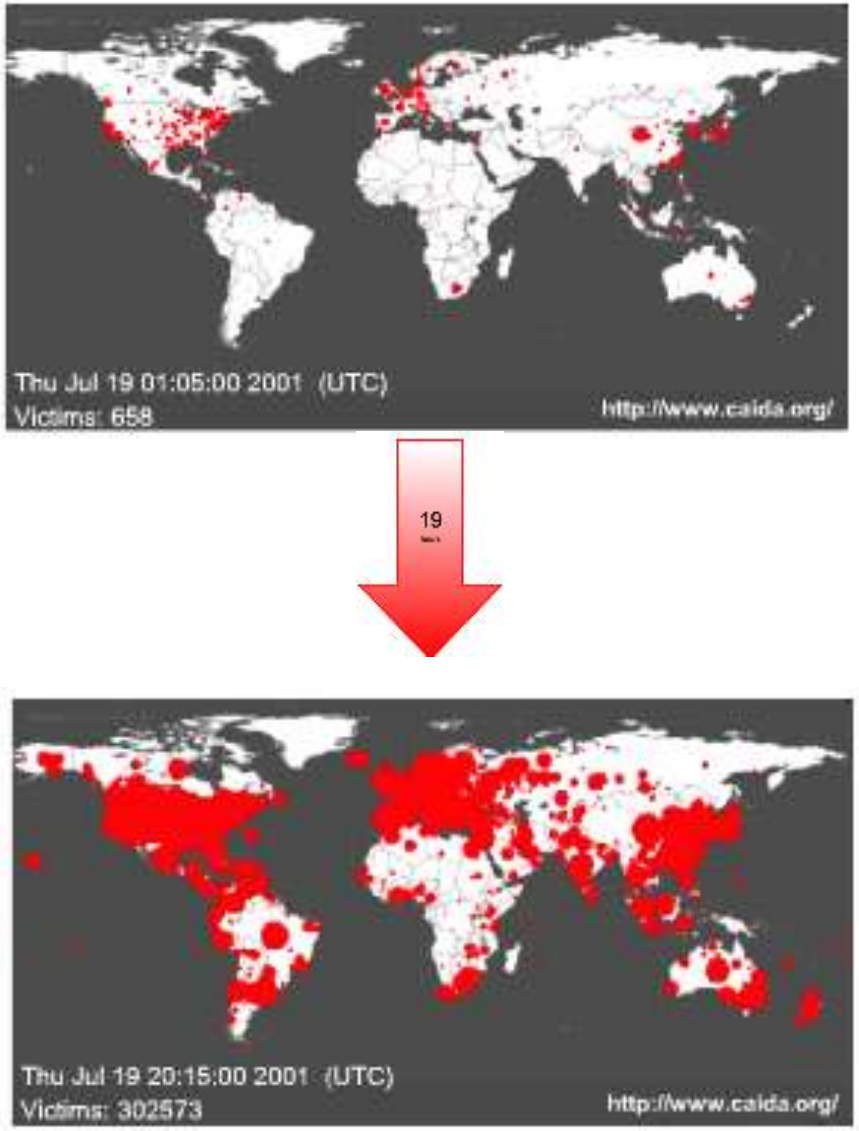
- Cheval de Troie pour l’accès distant
  - Permet l'accès à distance non autorisé
- Cheval de Troie pour l’envoi des données
  - Fournit à l'attaquant des données sensibles telles que des mots de passe
- Cheval de Troie destructeur
  - Corrompt ou supprime des fichiers
- Cheval de Troie Proxy
  - L'ordinateur de l'utilisateur fonctionne comme un serveur proxy
- Cheval de Troie FTP (ouvre le port 21)
  - Logiciel de sécurité Disabler Cheval de Troie (arrête les programmes anti-virus ou les pare-feu de fonctionnement)
- Cheval de Troie de déni de service (ralentit ou interrompt l'activité réseau)

Vers

- Les vers sont un type particulièrement dangereux de code.
  - Ils se répliquent en exploitant indépendamment les vulnérabilités des réseaux.
  - Les vers ralentissent habituellement les réseaux.
- Les Vers N'ONT PAS BESOIN DE L'INTERVENTION DE L'UTILISATEUR!
  - Les vers, ne nécessitent pas la participation des utilisateurs et peuvent se propager extrêmement rapidement sur le réseau.

SQL Slammer Worms

- En juillet 2001, le SQL Slammer Worm a ralenti le trafic Internet global à la suite de DoS.
- Plus de 250 000 hôtes ont été touchés dans les 30 minutes suivant sa sortie.
- Le ver a exploité un bogue de dépassement de capacité dans Microsoft SQL Server.
  - Un correctif pour cette vulnérabilité a été publié au milieu de 2001, donc les serveurs affectés étaient ceux qui n'avaient pas le patch de mise à jour appliqué.



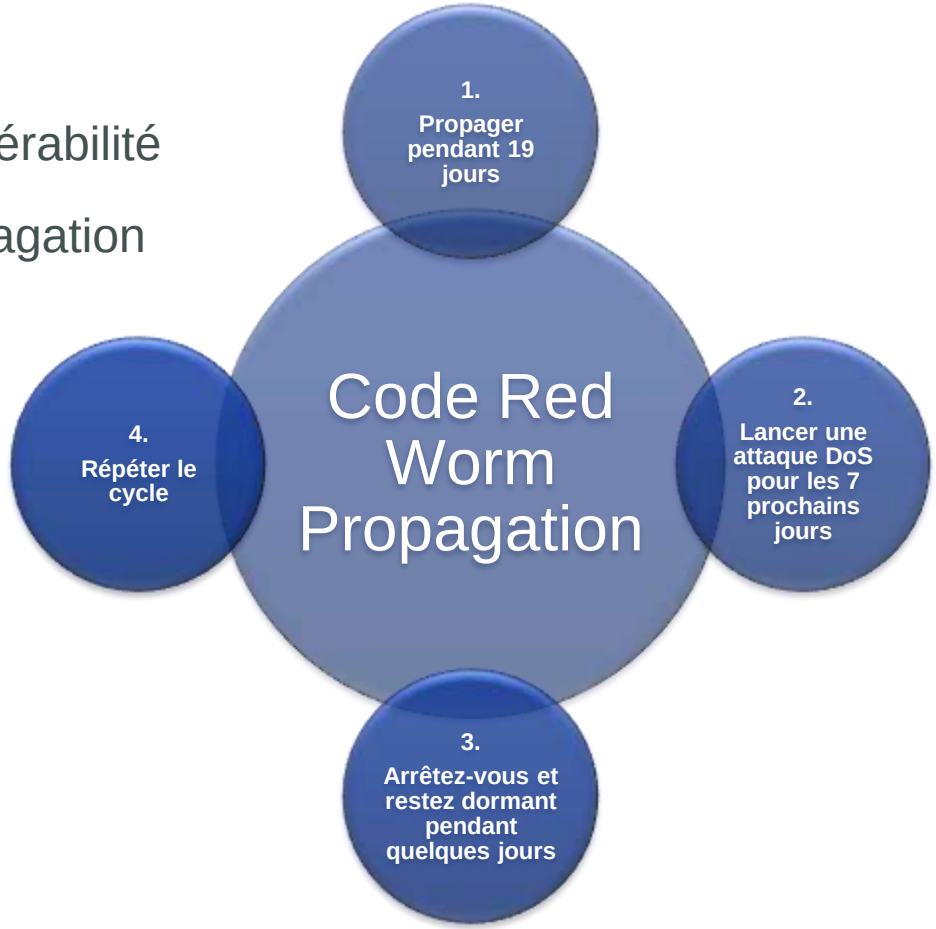
Anatomie d'un ver

- La vulnérabilité d'activation
  - Un ver s'installe à l'aide d'un vecteur d'exploit sur un système vulnérable.
- Mécanisme de propagation
  - Après avoir accédé aux périphériques, un ver réplique et sélectionne de nouvelles cibles.
- Charge utile
  - Une fois que le dispositif est infecté par un ver, l'attaquant a accès à l'hôte - souvent en tant qu'utilisateur privilégié.
- Les attaquants pourraient utiliser un exploit local pour escalader leur niveau de privilège à l'administrateur.

Composants de ver

Composants:

- Activation de la vulnérabilité
- Mécanisme de propagation
- Charge utile



•**Ransomware** - Ce logiciel malveillant refuse l'accès au système informatique infecté. Le rançon exige alors une rançon payée pour que la restriction soit supprimée.

•**Spyware** - Ce logiciel malveillant est utilisé pour recueillir des informations sur un utilisateur et envoyer les informations à une autre entité, sans le consentement de l'utilisateur.

•**Adware** - Ce malware affiche généralement des pop-ups ennuyeux pour générer des revenus pour son auteur. Le logiciel malveillant peut analyser les intérêts des utilisateurs en suivant les sites Web visités.

•**Scareware** - Ce logiciel malveillant comprend un logiciel d'arnaque qui utilise l'ingénierie sociale pour choquer ou induire l'anxiété en créant la perception d'une menace. Il est généralement dirigé vers un utilisateur non méfiant.

•**Phishing** - Ce malware tente de convaincre les internautes de divulguer des informations sensibles. Les exemples incluent recevoir un email de leur banque demandant aux utilisateurs de divulguer leur compte et NIP.

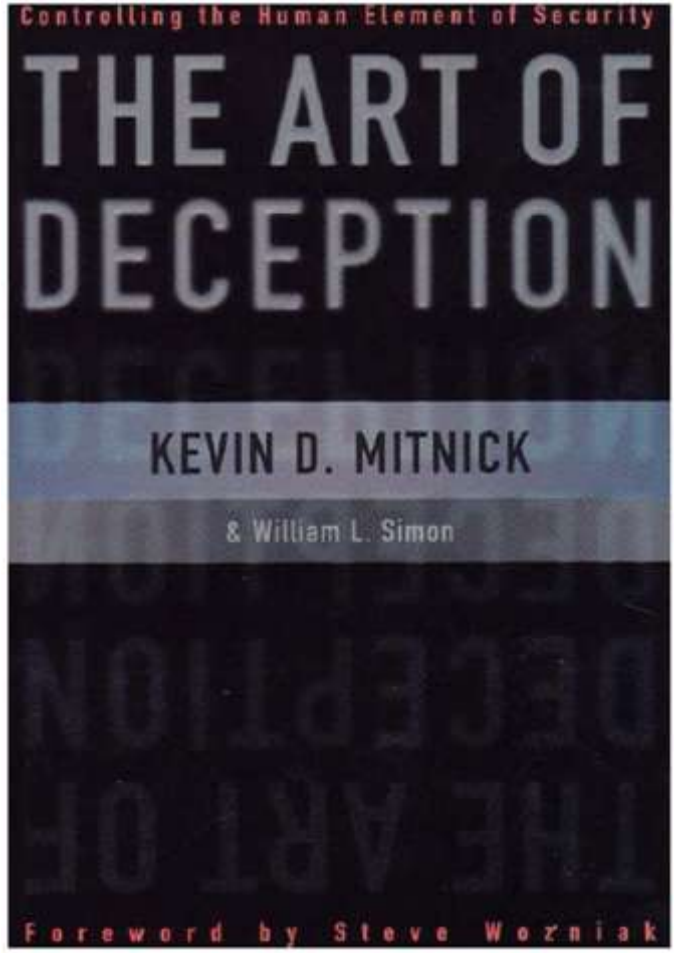
•**Rootkits** - Ce malware est installé sur un système compromis. Après son installation, il continue à cacher son intrusion et à maintenir un accès privilégié au hacker.

Etape 3 - Manipuler les utilisateurs pour obtenir un accès

- L'ingénierie sociale est un moyen de manipuler les personnes à l'intérieur du réseau pour fournir les informations nécessaires afin d'accéder au réseau.
  - ❑ Un ordinateur n'est pas nécessaire !!
  - ❑ Ingénierie sociale par téléphone
  - ❑ Dumpster plongée
  - ❑ Ingénierie sociale inversée
- Lecture recommandée:

✓ *"L'art de la supercherie (The Art of Deception) "*

Mitnik, KD et Simon, WL; Wiley; Nouvelle édition Ed



Travail a faire

Example #1 Social Engineering

- Call in the middle of the night:
  - ‘Hi this is _____ from Bell. I’m very sorry to wake you up but we’ve noticed some very unusual activity on your Bell calling card and we’re wondering if you’re using it to call Baghdad, Iraq for the last 6 hours?’
  - ‘Well, we have a call that’s actually still active right now and it’s now well over $2,000 worth of charges. I’ll terminate that call right now but unfortunately you are responsible for the charges made on your card.’
  - ‘Look I sympathize with you and can see that you’ve been victimized here, but if I get rid of that charge I can loose my job.’
  - ‘Okay … but you’ll have to confirm some details first. What is your full name and address?’
  - ‘Can you confirm the Bell calling card number?’
  - ‘Finally, please confirm your PIN number?’
  - ‘Great. Everything matches. I’ll get rid of that charge for you.’
  - ‘You’re welcome and thank you for being a Bell Canada client.’

Example #2 Social Engineering

- Un expert d'un institut de sécurité informatique a clairement illustré la vulnérabilité des bureaux d'assistance en direct quand il a "appelé" une compagnie de téléphone, il a été transféré autour, et a atteint le help desk:

- ‘Who’s the supervisor on duty tonight?’
  - ‘Let me talk to _____.’ (he’s transferred)
  - ‘Hi _____, this is _____ from security in the IT center. Having a bad day?’
  - ‘No, why?...Your systems are down.’
    - Response: ‘my systems aren’t down, we’re running fine.’
  - ‘Hmmm … Really? Do me a favor then and sign off and on again.’
  - ‘We didn’t even show a blip, we show no change. Sign off again.’
  - ‘There’s something funny going on here. I’m going to have to sign on with your ID to figure out what’s happening. Let me have your user ID and password.’

Signes d'avertissement d'une attaque

- Refus de donner le numéro de rappel
- Demande non ordinaire
- Demande d'autorisation
- Souligne l'urgence
- Menace les conséquences négatives de la non-conformité
- Montre de l'inconfort lorsqu'il est questionné
- Nom qui tombe
- Compliments ou flatteries

Les Principes de conception de sécurité réseau

» Politiques de sécurité

Premier et le plus important

Comment un utilisateur peut-il se comporter de façon appropriée sans une politique en place pour cela ?

Comment un utilisateur peut-il savoir ce qui est permis et interdit ?

Comment pouvez-vous blâmer un utilisateur de ne pas savoir quelque chose qu'il n'a pas été dit ?

- Nous avons des politiques techniques et des politiques utilisateur

» Défense-Profondeur

- Ne signifie pas redondance, mais approche en couches

» Segmentation réseau

- Groupement des biens du même type / valeur / niveau de risque dans des zones de sécurité

» Le moins de privileges

- Autoriser les utilisateurs et le système ayant accès uniquement à effectuer leurs tâches quotidiennes

Principes de conception de sécurité réseau

» Séparation des tâches

- Un utilisateur n'a pas de privilège de niveau 15 sur un périphérique et aussi pour le Système d'audit de commande

» Liens les plus faibles

- Votre réseau est aussi sûr que votre lien le plus faible
- Les humains sont considérés comme le maillon le plus faible, ils peuvent être manipulés
  - ❑ En utilisant d'autres principes, le risque peut être réduit

» Responsabilisation et non-répudiation

- L'activité de l'utilisateur doit être comptabilisée et vérifiée, utile pour l'analyse de la forensics
- Les données recueillies doivent présenter des preuves comme n'étant pas falsifiées

Other Social Engineering Examples

- Une personne confuse et troublée va appeler un employé et demande simplement un changement de mot de passe.
- Les personnes s'identifiant comme cadres, téléphonent à un nouvel administrateur système et demandent l'accès à leur compte IMMÉDIATEMENT!
- Quelqu'un va appeler et confidentiellement demande à un opérateur d'ordinateur pour taper quelques lignes d'instruction à la console.
- Dans un aéroport, quelqu'un regardera par-dessus une épaule, «surf à l'épaule» (parfois même en utilisant des jumelles ou des caméscopes), car les numéros de carte de crédit téléphonique ou les PIN ATM sont saisis.