Next Generation Secure Computing Base (NGSCB)

- Überblick -

Gerold Hübner
Chief Security Officer
Microsoft Deutschland GmbH

Agenda

- **Was** ist die Vision hinter Trustworthy Computing und NGSCB?
- **Warum ist** NGSCB wichtig?
- **Wie funktioniert** NGSCB?
- **Welche** Probleme löst NGSCB?
- **Wann** ist NGSCB verfügbar?

Trustworthy Computing

Sicherheit

- Angriffen widerstehen
- Schutz der Vertraulichkeit, Integrität, Authentizität und Verbindlichkeit

Datenschutz

- Benutzer hat Daten unter Kontrolle
- Produkte und Onlinedienste halten Datenschutzbestimmungen ein

Hochverfügbarkeit

- Zuverlässigkeit
- Daten sind verfügbar wenn gebraucht
- Einhaltung von Service Levels

Integrität

- Kunden bekommen die Lösungen, die sie brauchen
- Probleme bei Produkten und Dienstleistungen werden behoben
- Offene Interaktion mit Kunden

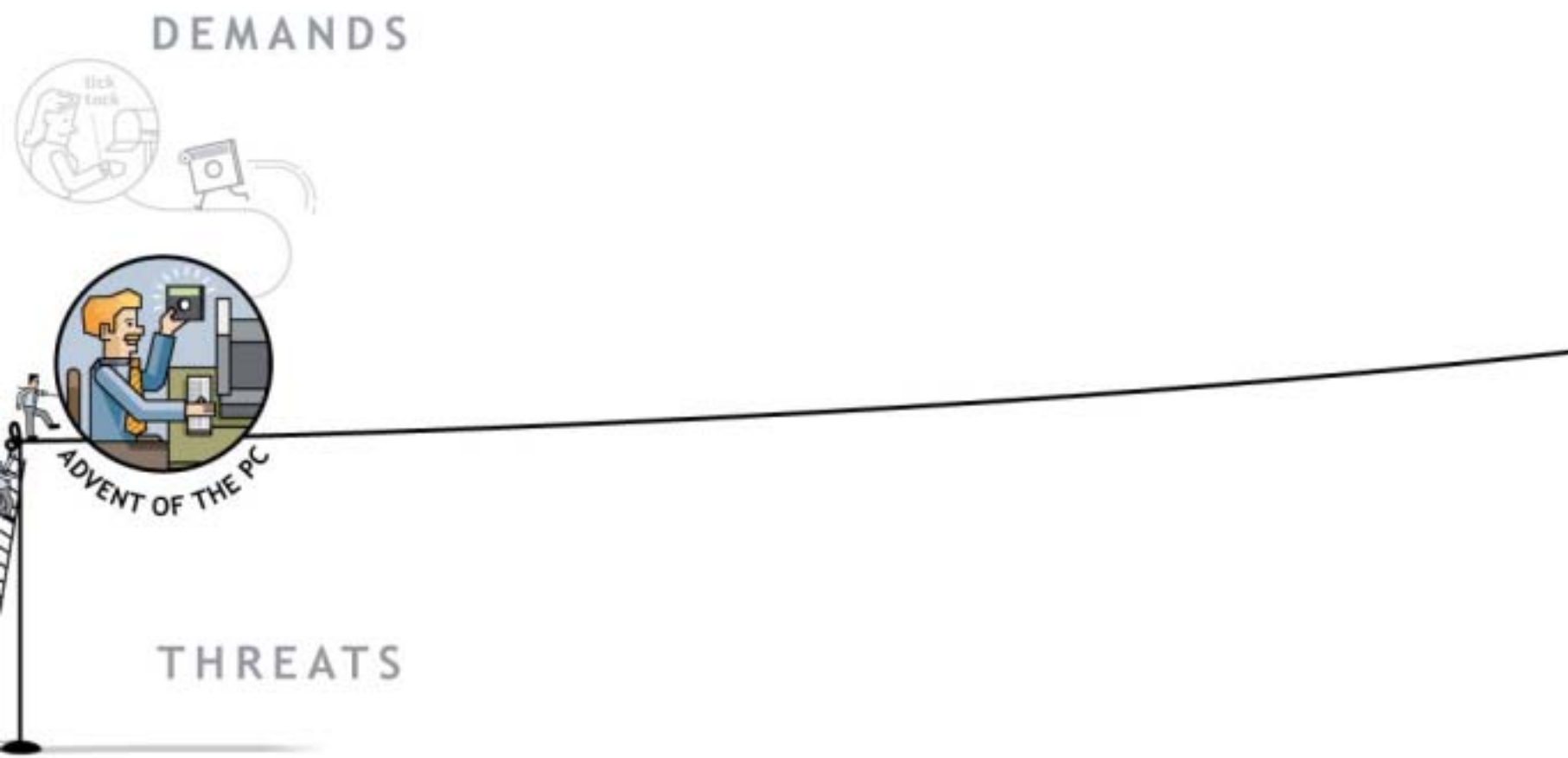
Next Generation Secure Computing Base (Definition)

NGSCB ist eine neue Sicherheitstechnologie für die Microsoft Windows Plattform, die auf einem innovativen neuen Design miteinander kombinierter Hard- und Softwareelemente beruht und Anwendern neue Mechanismen für mehr Sicherheit und Datenschutz in einer vernetzten Welt zur Verfügung stellt.

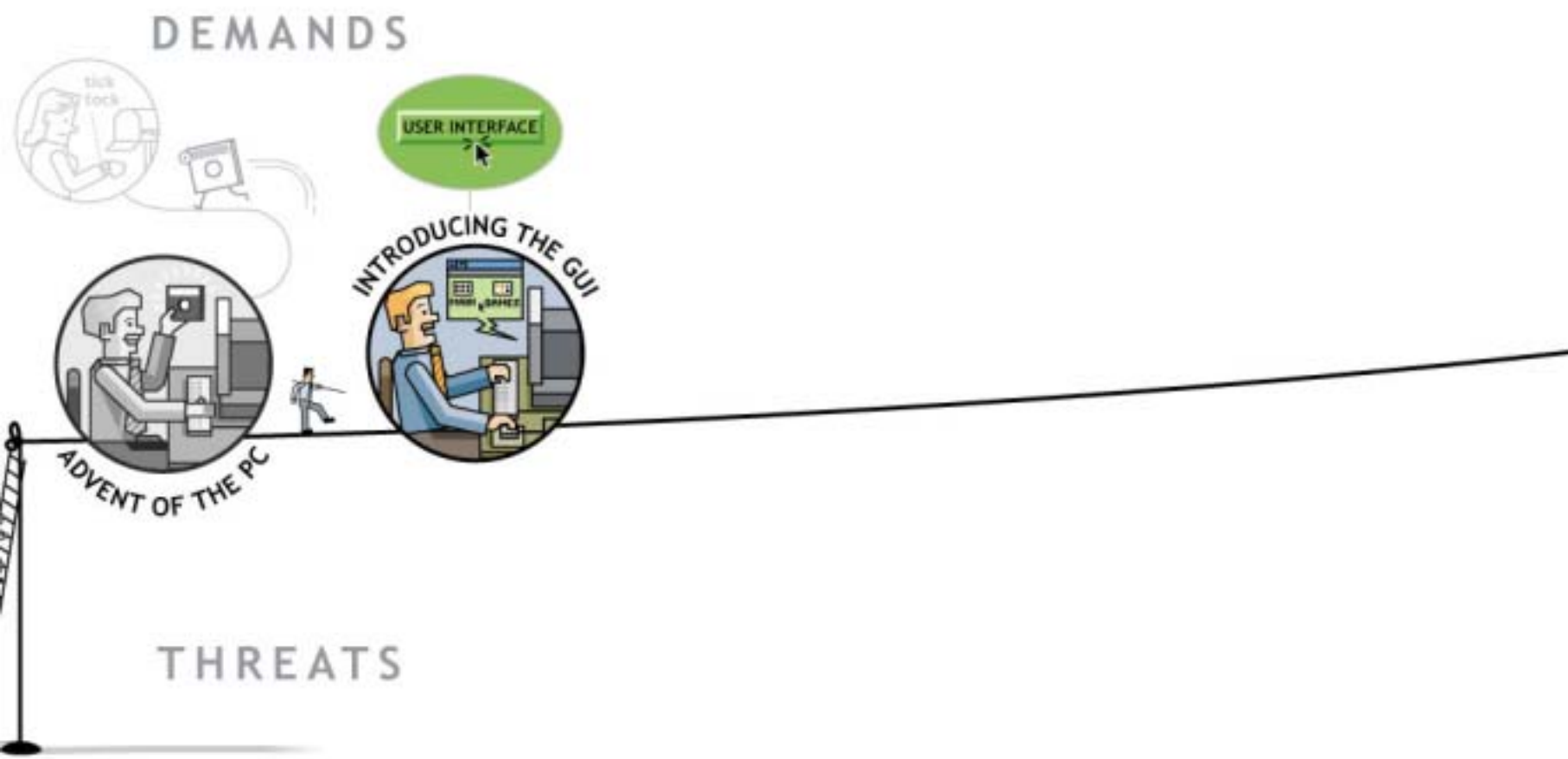
NGSCB – Vision und Ziele

- **Vision**
  - NGSCB erlaubt die Weiterentwicklung PC-basierter Geschäftsmodelle mit neuen Anforderungen an Sicherheit und Datenschutz
- **Produktziel**
  - NGSCB wird PCs so sicher wie "geschlossene Systeme" machen ohne auf die Flexibilität der Windows Plattform verzichten zu müssen
- **Business-Ziel**
  - NGSCB wird neue Hard- und Softwareprodukte ermöglichen und so helfen den IT-Markt wieder anzukurbeln

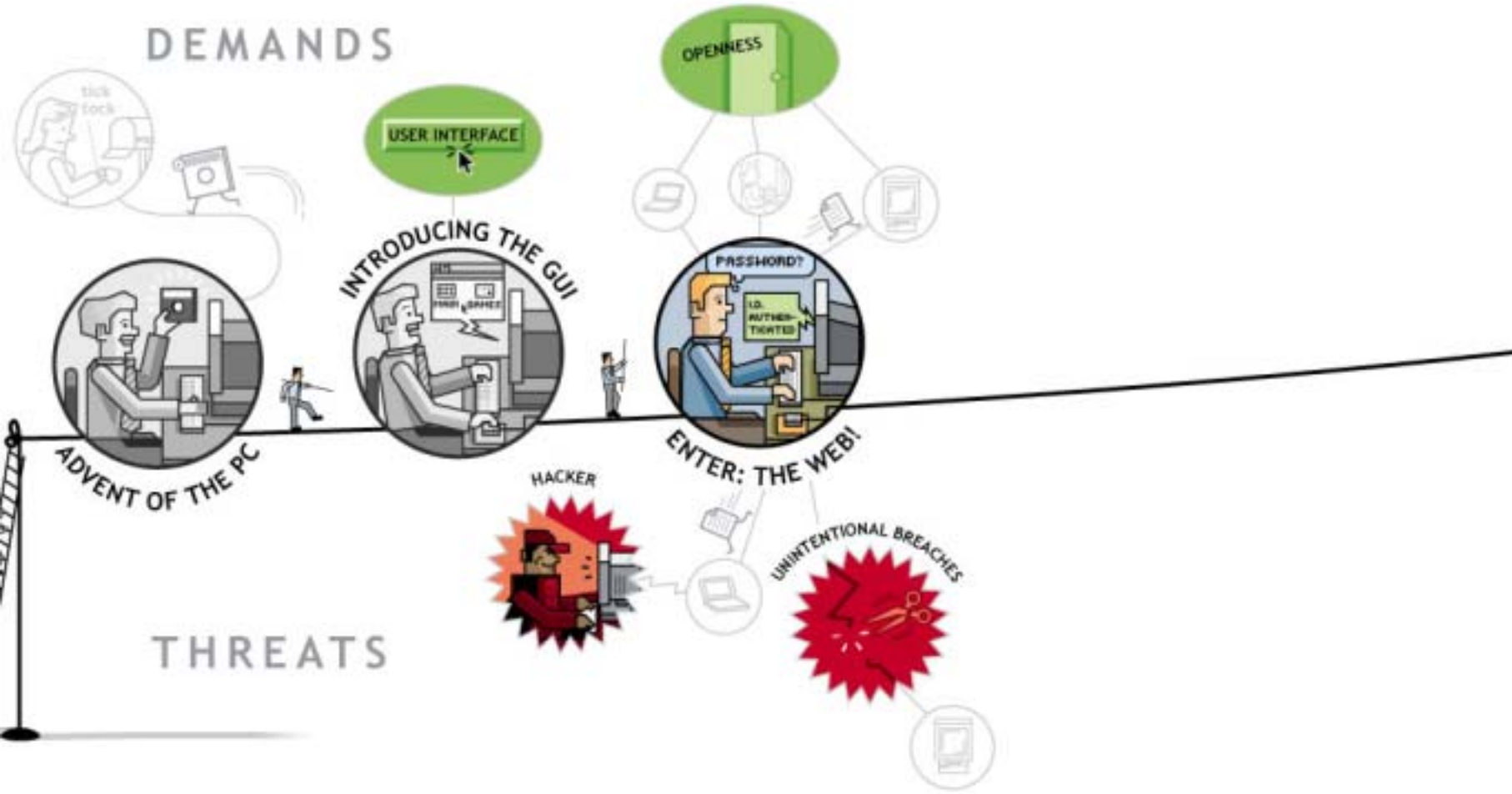
Anforderungen und Bedrohungen: Ein Drahtseilakt



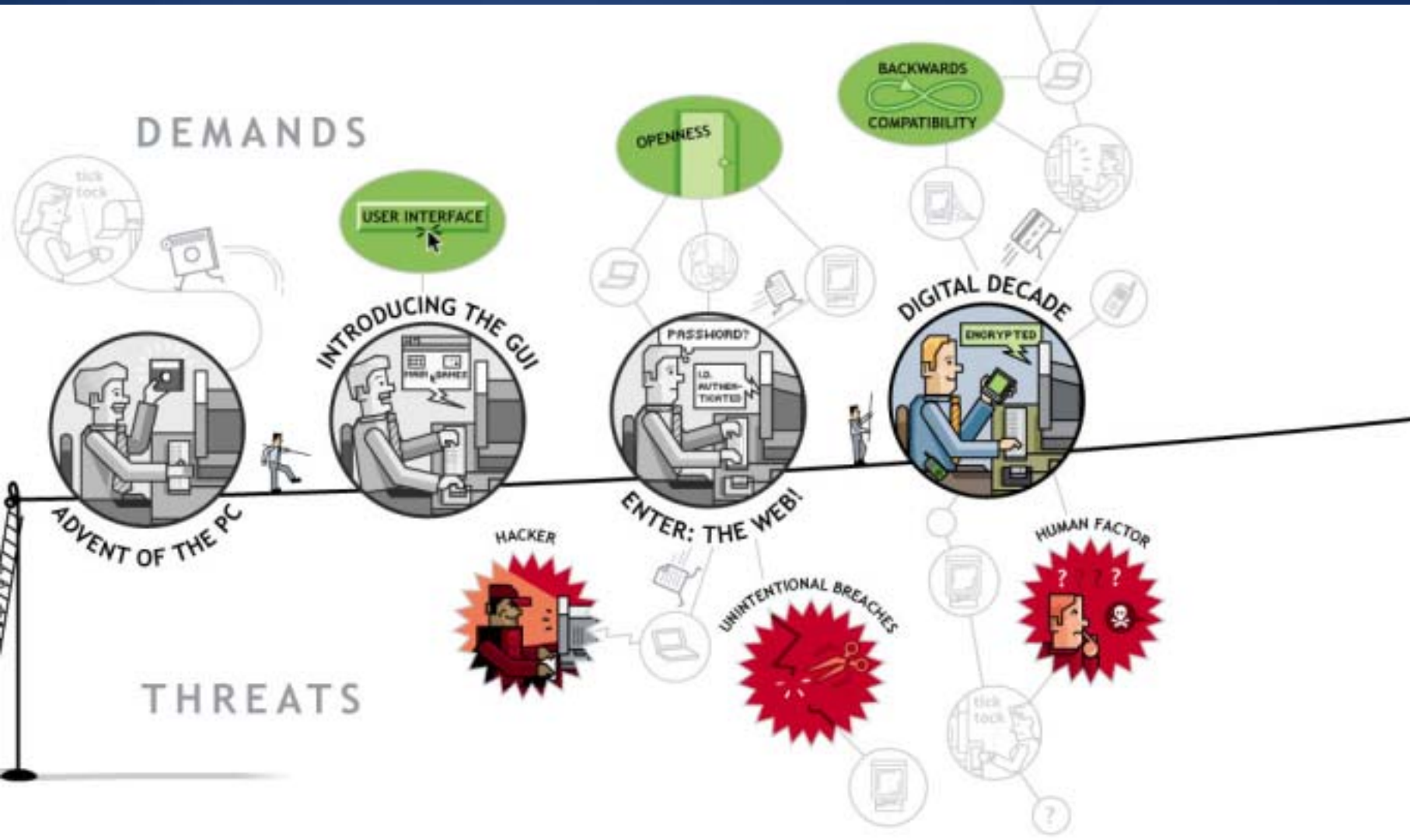
Anforderungen und Bedrohungen: Ein Drahtseilakt



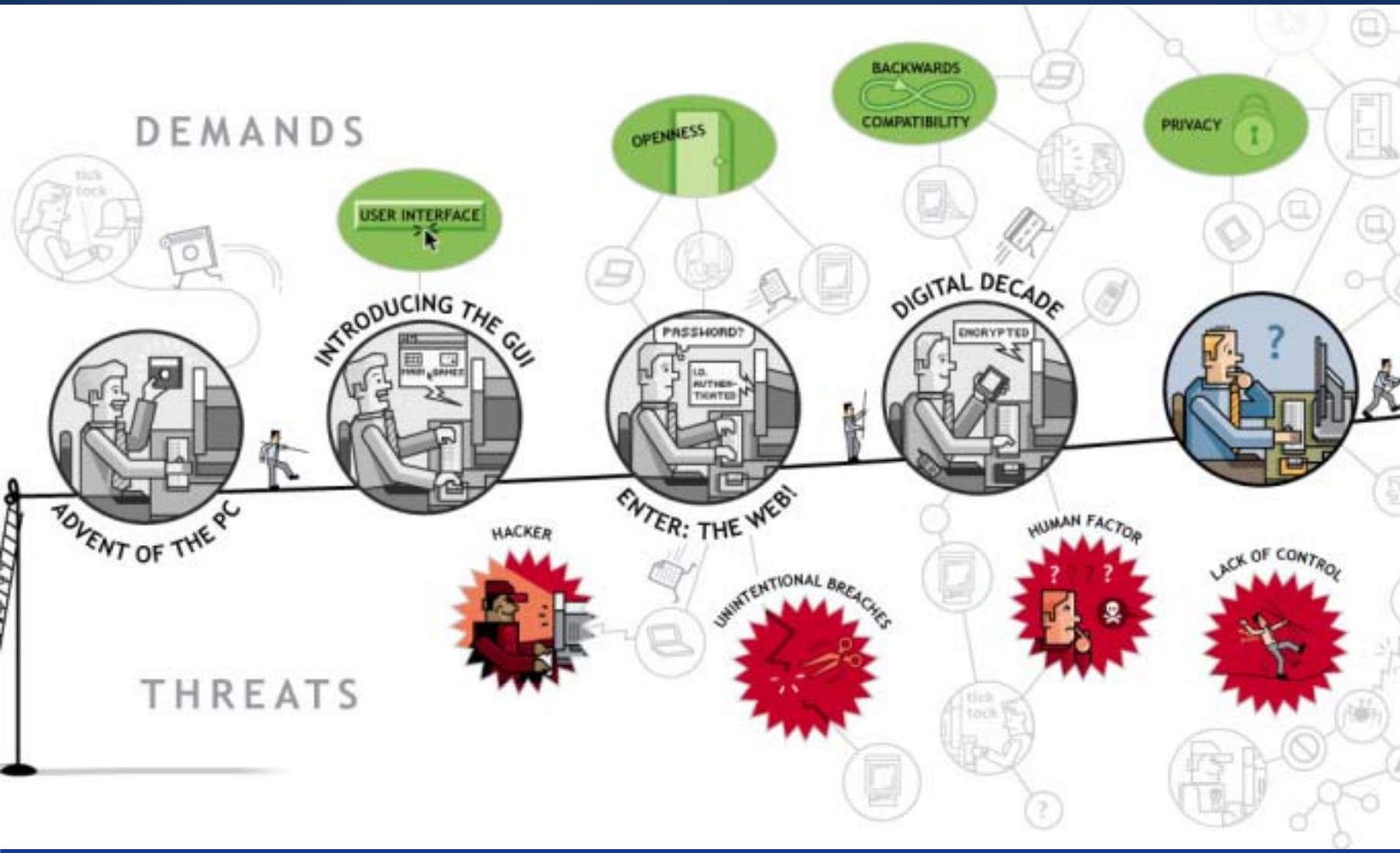
Anforderungen und Bedrohungen: Ein Drahtseilakt



Anforderungen und Bedrohungen: Ein Drahtseilakt



Anforderungen und Bedrohungen: Ein Drahtseilakt



Herausforderung Sicherheit

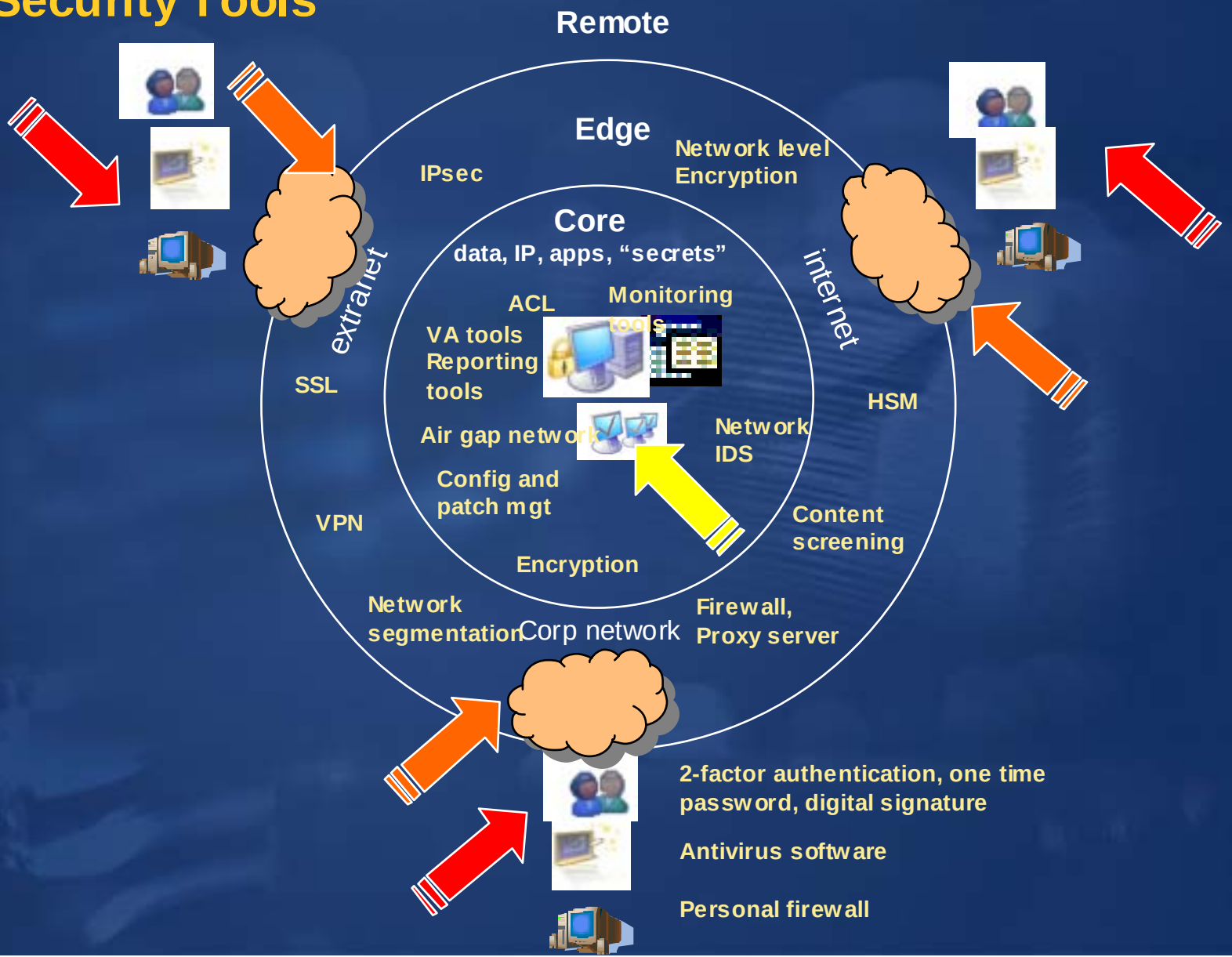
- Zunehmende Vernetzung erhöht die Sicherheitsanforderungen
  - Kritische Infrastrukturen, z.B.
    - Telekommunikation
    - Banken
    - Energieversorger
  - E-Business, E-Government
  - Innere Sicherheit
  - Datenschutz

- Voraussetzung für die Entwicklung der Informations- und Wissensgesellschaft ist Vertrauen in neue Technologien!

Zunehmende Vernetzung und Inflation der Angriffe

Anzahl der "Vorfälle" beim CERT Coordination Center (www.cert.org) pro Jahr

Taxonomy der IT-Ressourcen, Bedrohungen und Security Tools



Was ist zu tun?

- Klassische Sicherheitskonzepte stossen an ihre Grenzen
  - Komplexität von Sicherheitslösungen immer schwerer beherrschbar
  - immer größeres Missverhältnis zw. Aufwand und Nutzen
  - Von reiner Abwehrfunktion zum “Business Enabler”
- Anwender wollen Flexibilität und Vielfalt heutiger PC-Architekturen als auch Sicherheit und Vertrauen in ihre PCs

Die Probleme der Anwender

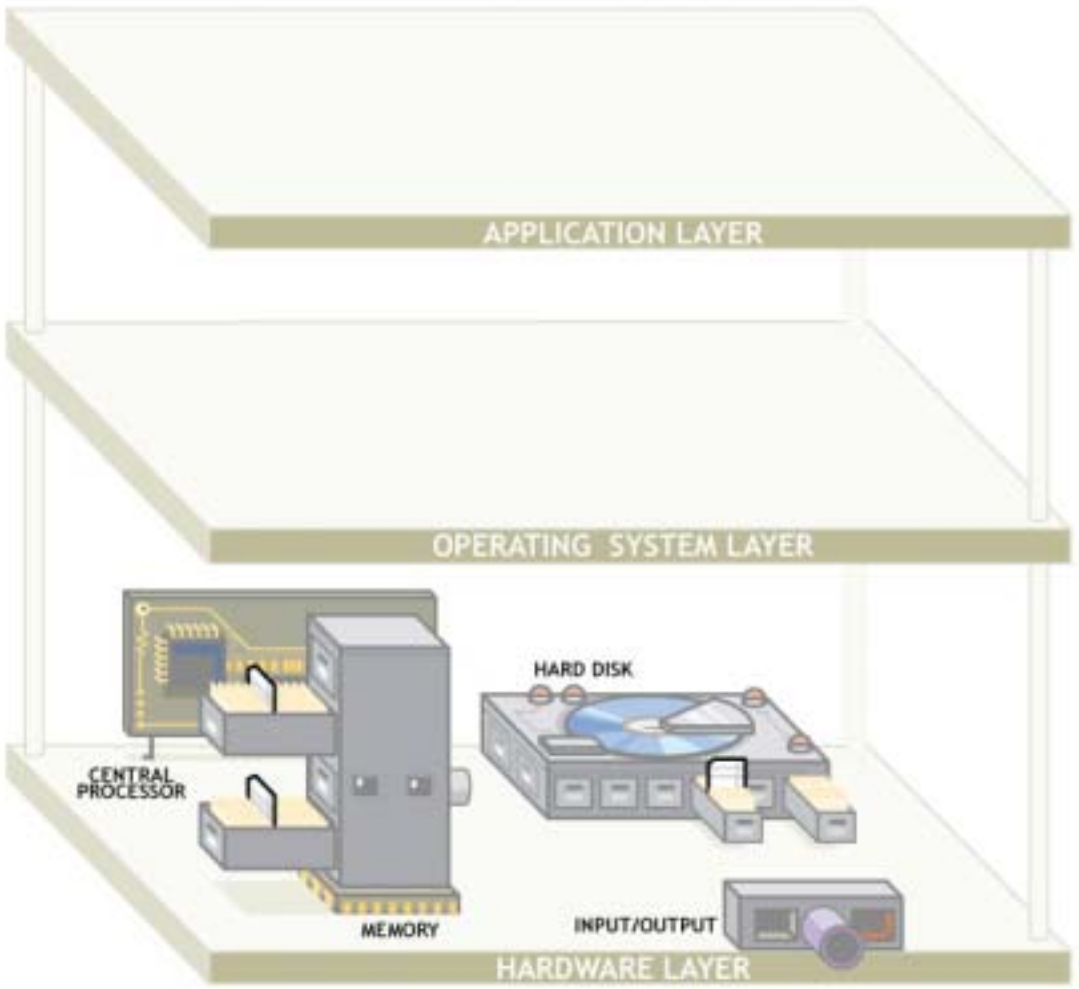
- Remote Zugang öffnet Netze
- Unberechtigter Zugriff auf und illegale Nutzung sensibler Informationen
- Schwierig festzustellen wer wirklich am an anderen “Ende der Leitung” ist
- Patch Management schwer zu beherrschen
- Sonstige Herausforderungen:
  - Zusammenarbeit in sicheren Netzen
  - Schutz von System-Geheimnissen, z. B. kryptografisches Material wie Schlüssel, Zertifikate, Hashwerte
  - Abwehr von Schadprogrammen (Viren etc.)

Die Rolle der NGSCB

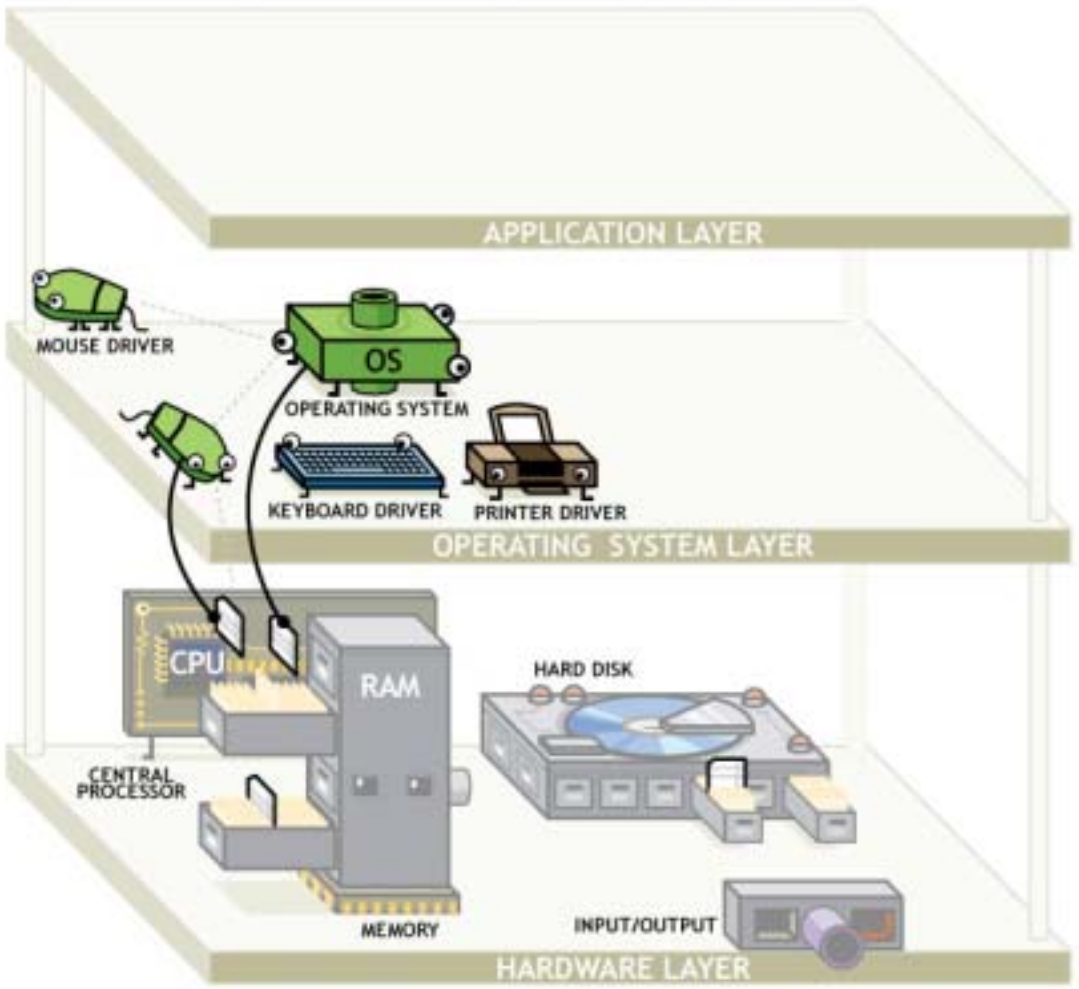
- Technisch und wirtschaftlich schwierig bis unmöglich Angriffe auf
  - zentrale IT-Ressourcen
  - Netzwerke
  - Remote User und Maschinen

  zu verhindern
- NGSCB kann Schäden durch Sicherheitsverletzungen kontrollieren und/oder limitieren

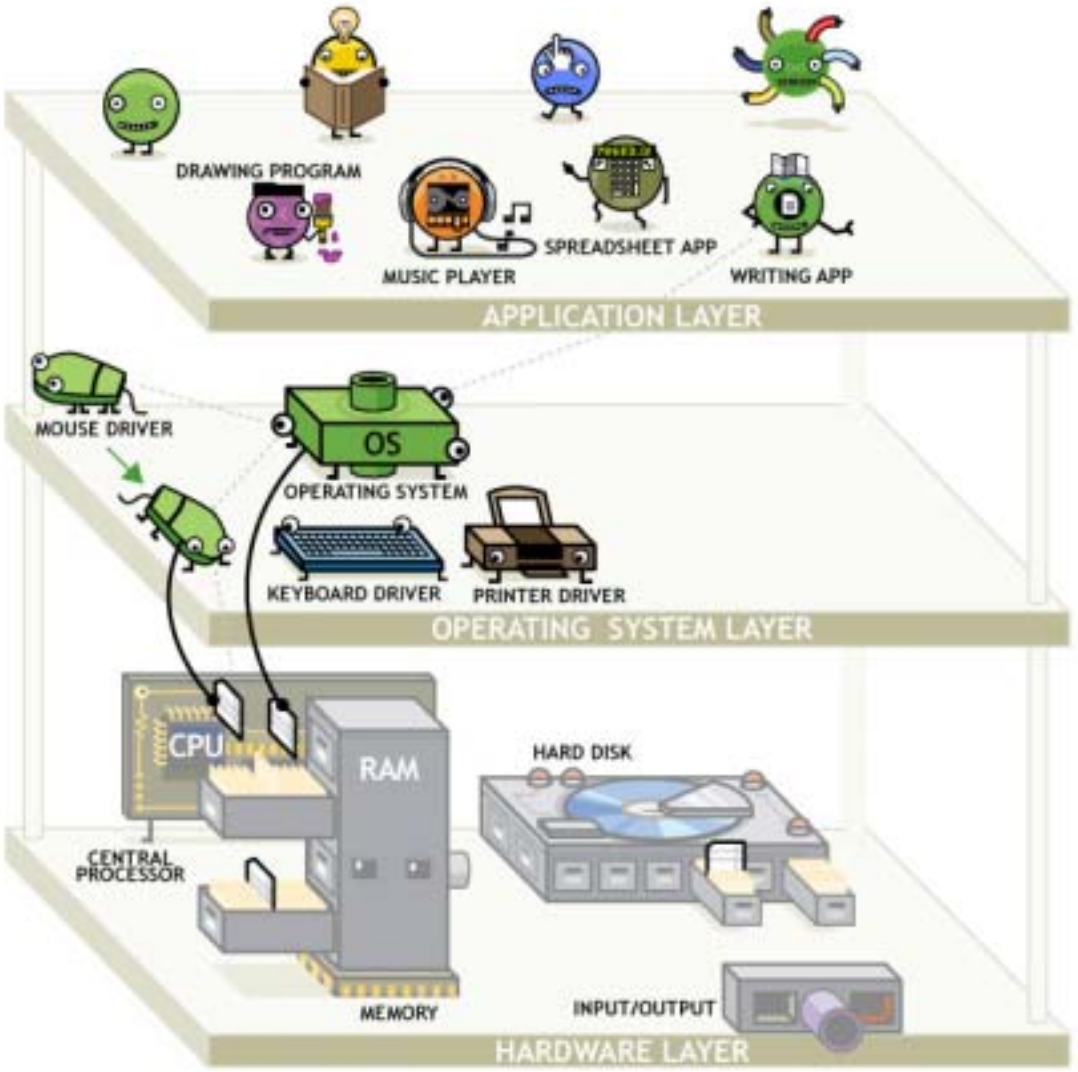
So funktioniert's: Der PC



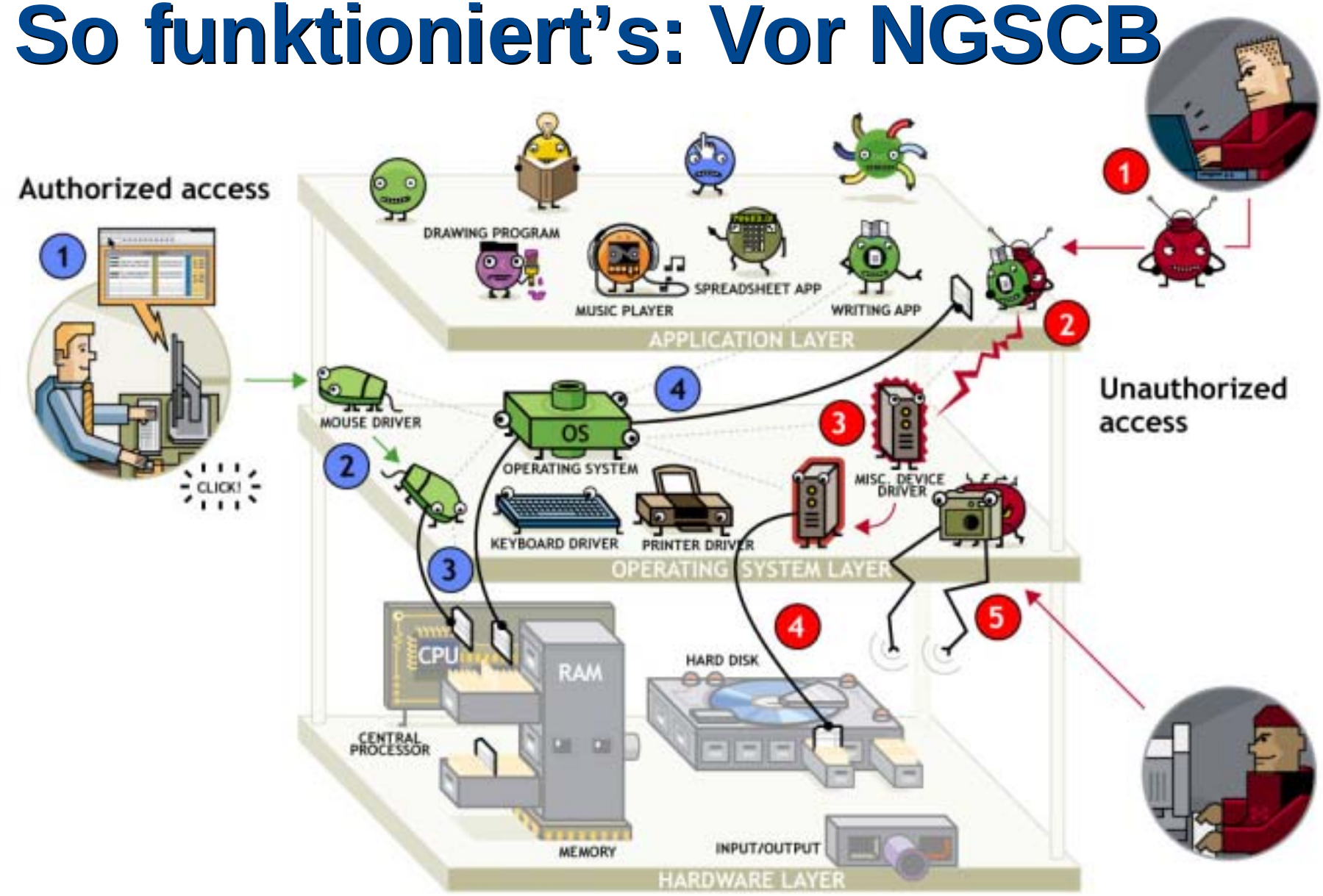
So funktioniert's: Vor NGSCB



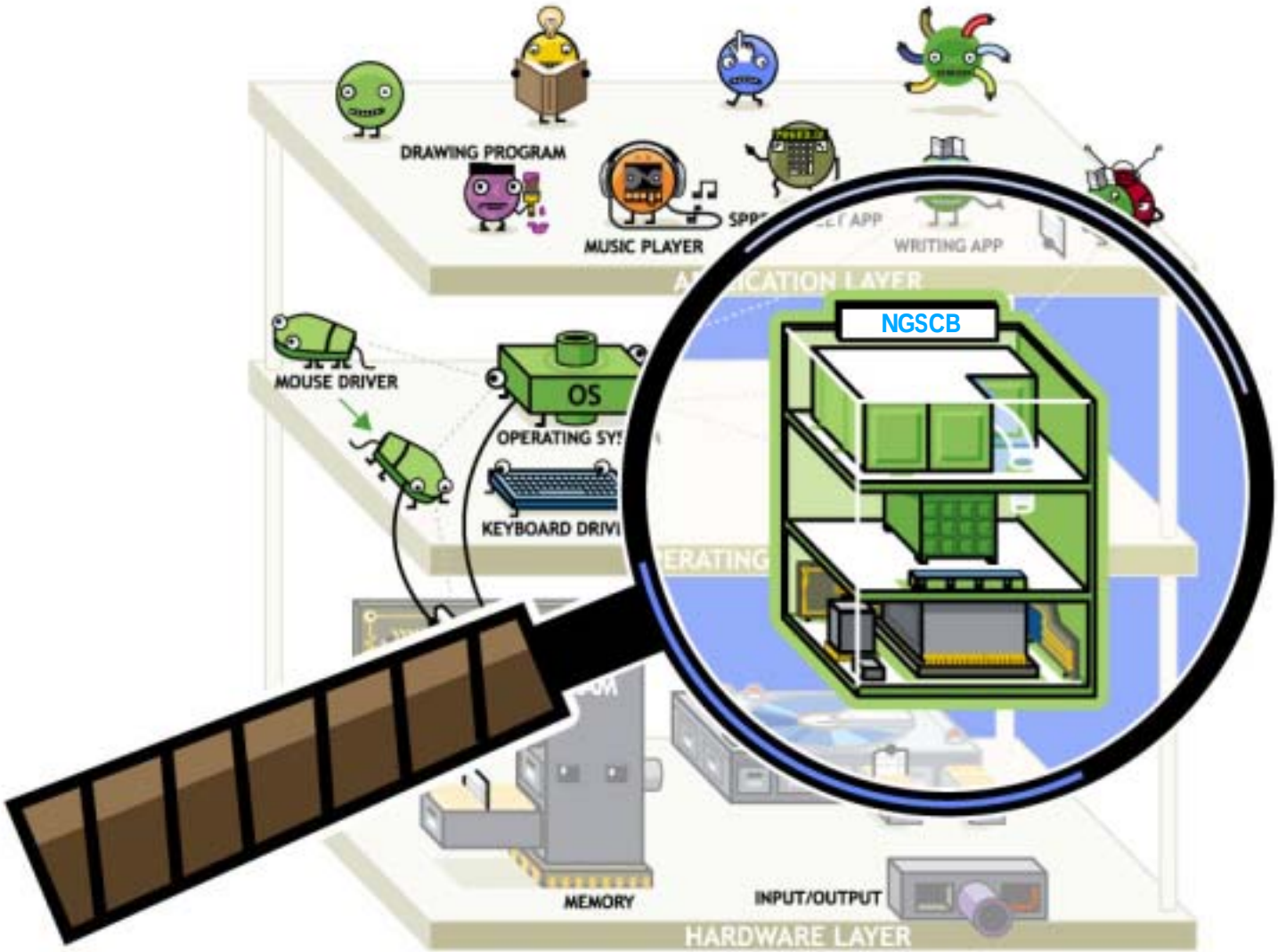
So funktioniert's: Vor NGSCB



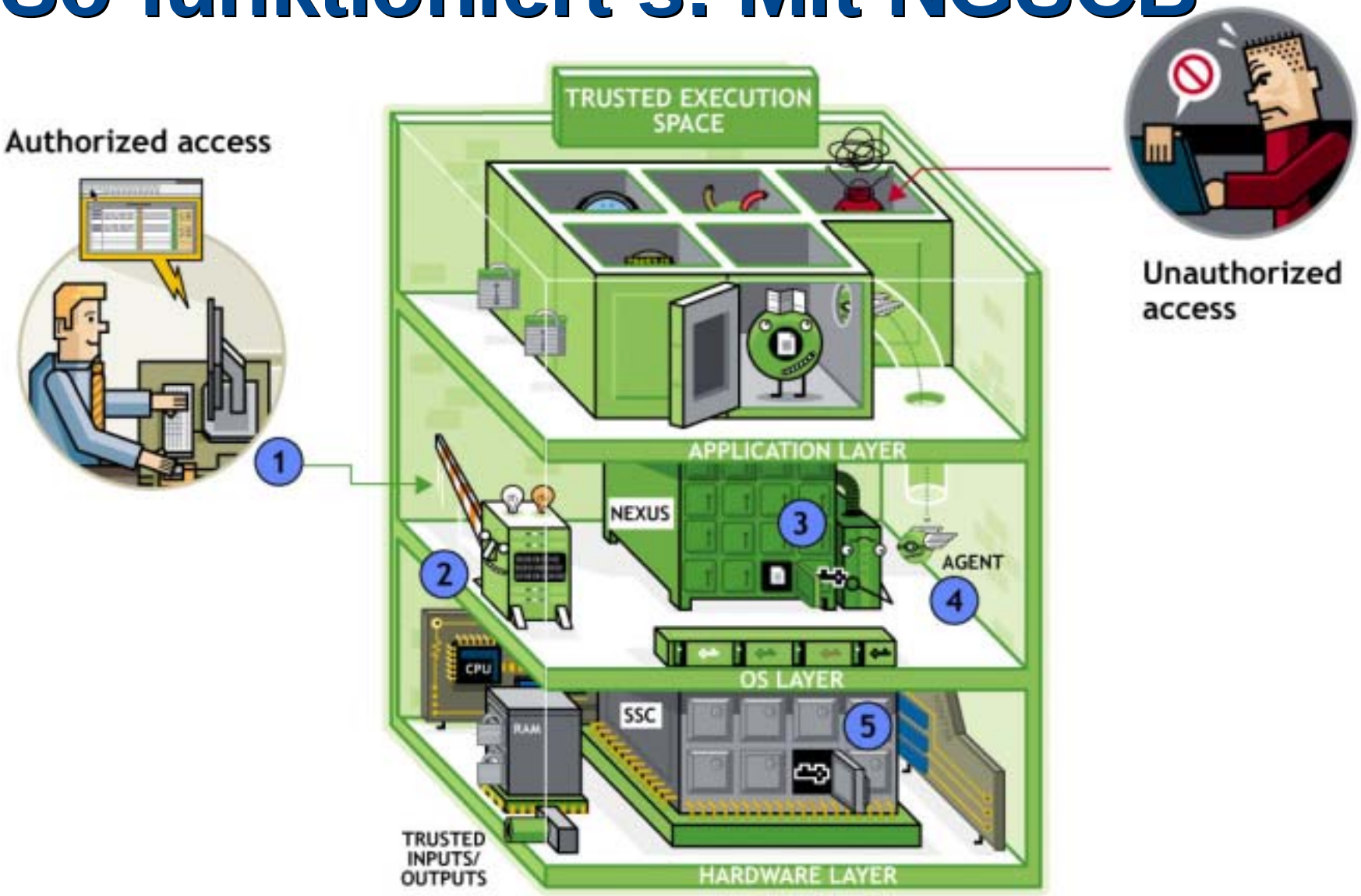
So funktioniert's: Vor NGSCB



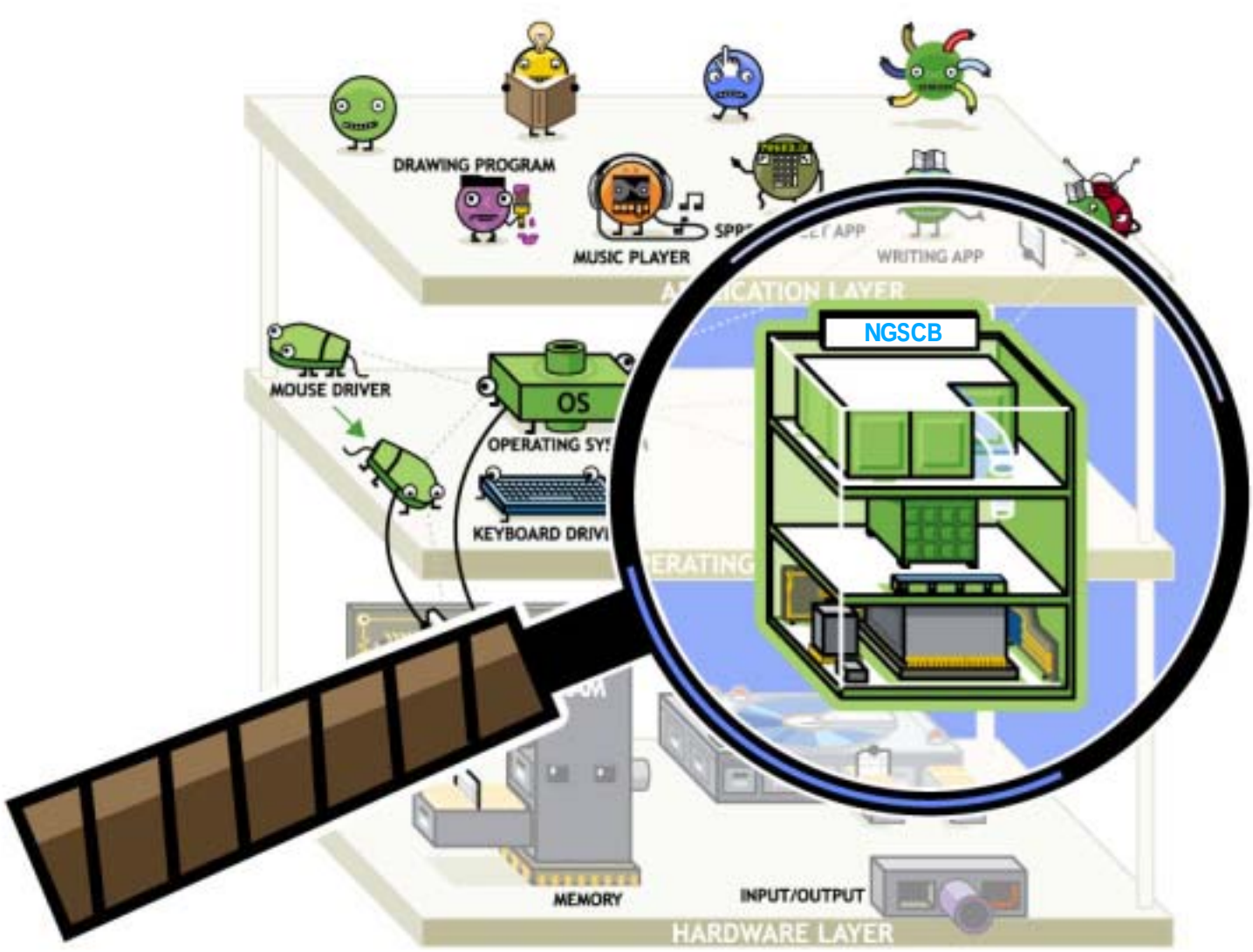
So funktioniert's: Vor NGSCB



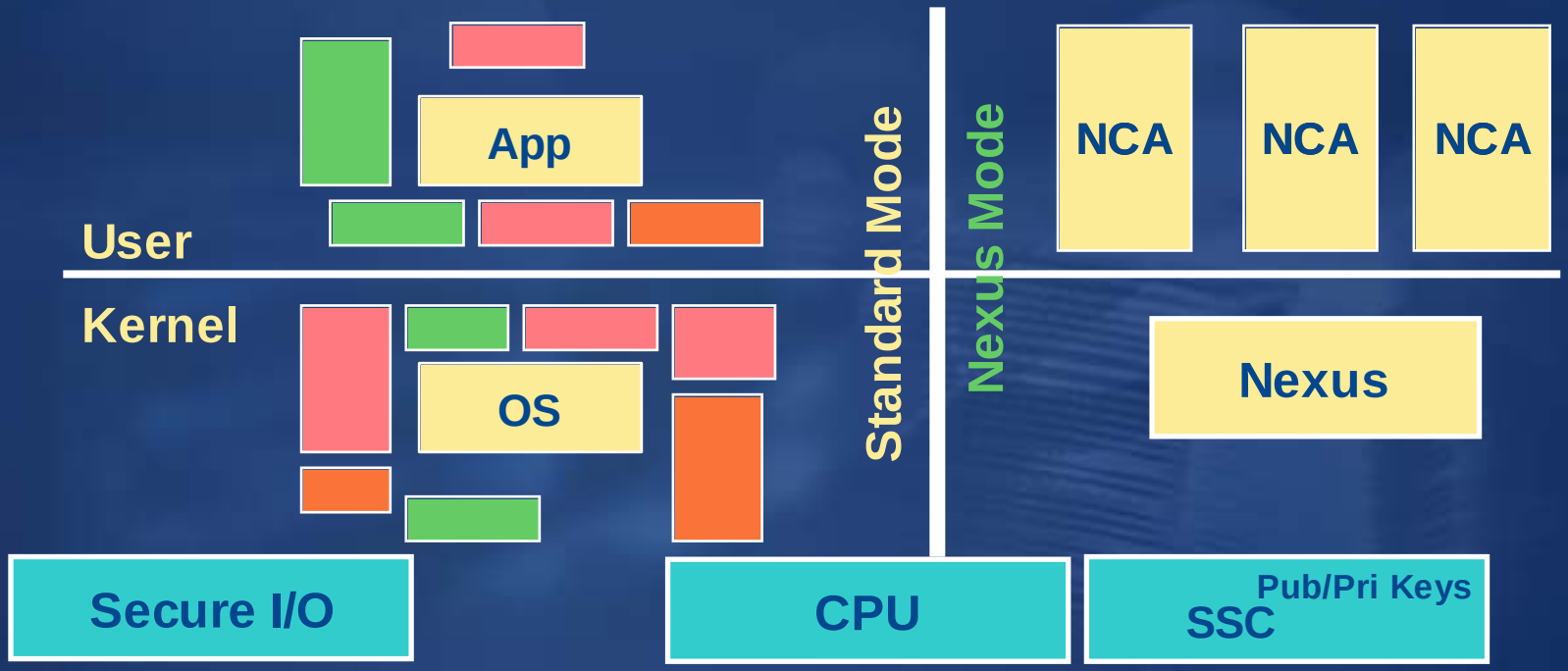
So funktioniert's: Mit NGSCB



NGSCB – anders Betrachtet . . .



NGSCB und die vier Quadranten



Vier NGSCB Basis-funktiontionalitäten

1. **Geschützter Speicherbereich (Curtained Memory)**
   - NGSCB-Applikationen vor potentiellen Schadprogrammen abschirmen
2. **Sicherer Speicherbereich (Sealed Storage)**
   - Sichere Ablage für sensible Daten
3. **Abgesicherte Ein- und Ausgaben (Trusted I/O)**
   - lückenloses Vertrauen von Tastatur/Maus bis zum Bildschirm
4. **Software Authentifizierung (Attestation)**
   - Aufbau von Vertrauensbeziehungen in verteilten Umgebungen (z. B. für E-Banking)

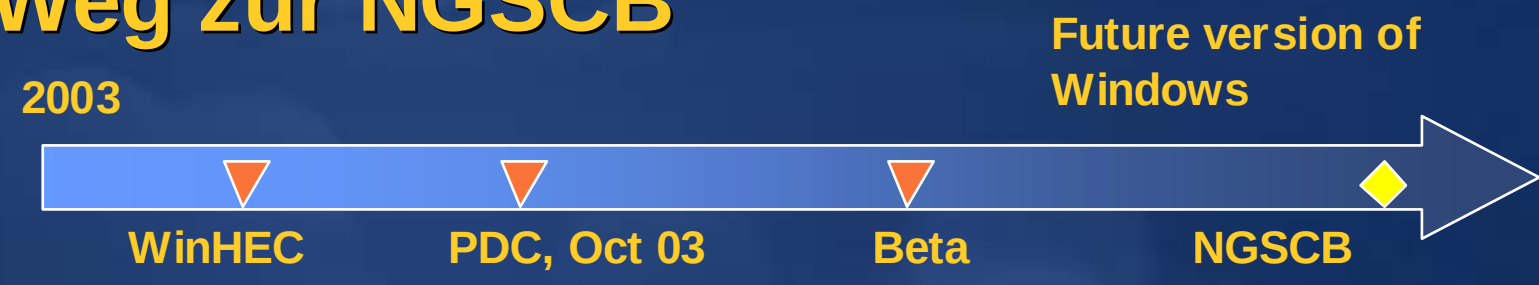
NGSCB Fakten

- Benutzer haben volle Kontrolle ob sie NGSCB nutzen wollen
  - NGSCB-fähige PC kommen mit NGSCB „off“
- Sämtliche heutige Software ist weiter nutzbar
- Programmierschnittstellen für NGSCB werden veröffentlicht und dokumentiert
  - Jeder kann NGSCB-Programme entwickeln!
- Der Microsoft-Nexus wird zur Evaluierung zur Verfügung stehen
- Keine Zertifizierung von NGSCB-Software nötig
  - keine zentrale Zertifizierungsinstanz
- NGSCB Systeme werden die Privatsphäre von Nutzern besser schützen als heutige PCs

Easing Customer Pains with NGSCB

- Remote access
  - Granularity of access at machine, nexus, and application level
  - Application to application connection rather than VPN connection
- Patch management
  - IT can specify that only a known configuration of nexus and application to execute or access corporate resources
- Preventing illegal access of information
  - Reinforce rights management by rooting key pair in hardware
  - Encryption of data based on secrets that never leave hardware
- Agents development
  - Agents identity is rooted in secrets on the hardware
  - Applications run in isolated process space and is impermeable to software attack
- Collaboration enablement
  - End users can collaborate and communicate securely
  - End users can establish content authenticity by digital signature

Der Weg zur NGSCB



NGSCB SDK	API Preview	Developer Preview (Pre-beta)	Beta SDK	SDK
NGSCB compliant HW	Standard x86 CPU	NA	NGSCB-ready desktop, laptop, and workstation	NGSCB Compliant hardware
Development Environment	None	Hardware with software emulator	Beta HW and complete SDK	NGSCB Compliant hardware

Weitere Infos:

- **Auf der NGSCB Homepage:**
  - http://www.microsoft.com/NGSCB
- **Newsgroup:**
  - http://communities.microsoft.com/newsgroups/default.asp?icp=ngscb&slcid=us
- **E-Mail Alias für Fragen zu NGSCB:**
  - ngscb_qa@microsoft.com

Microsoft®